UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

GRADO EN INGENIERÍA EN SISTEMAS DE COMUNICACIONES

MONITORIZACIÓN Y ANÁLISIS DEL TRÁFICO EN REDES INALÁMBRICAS 802.11

Trabajo Fin de Grado

Autor: Vicente Gaitán Garrido

Tutor: Pablo Serrano Yáñez-Mingot

Director: Carlos Jesús Bernardos Cano

Septiembre 2017

Agradecimientos

Llegado este momento me gustaría agradecer a mis padres por darme la oportunidad de estudiar una carrera así como por todo su apoyo durante estos años.

Agradecer también a mis tutores, Pablo y Carlos, por su ayuda y paciencia. Y por supuesto, a mis compañeros y amigos de universidad que me han acompañado durante el camino.

Índice General

Agradecimientos 3
Índice de figuras 7
Índice de tablas 9
Resumen 11
1. INTRODUCCIÓN 13
1.1. Contexto y motivación 13
1.2. Marco Regulador 17
1.2.1. Estándar de IEEE 802.11 18
1.2.2. Resoluciones de la CMT relacionadas con WIFI/Gestión del espectro 18
1.2.3. Ley de protección de datos 19
1.3. Productos similares 20
1.4. Objetivos 26
2. DESARROLLO DE LA SOLUCIÓN 28
2.1. Diseño del sistema 28
2.1.1. Descripción 28
2.1.2. Escenario 29
2.1.3. Componentes del sistema 32
2.2. Fundamentos de la solución 38
2.2.1. Consideraciones para la monitorización 38
2.2.2. Características del sistema 42
2.3. Implementación de la solución 43
2.3.1. Fase de captura 43
2.3.1.1. Objetivo 43
2.3.1.2. Datos de entrada a la fase de captura 44
2.3.1.3. Captura de la información 45
2.3.1.4. Estructura del programa 49
2.3.2. Fase de validación 61
2.3.2.1. Objetivo 61
2.3.2.2. Medidas 61
3. ANÁLISIS 64
3.1. Escenario 1 64
3.1.1. Análisis de comportamiento según la presencia de los dispositivos 64
3.1.2. Análisis de tráfico cursado por las redes 68

3.2. Escenario 2 70
3.2.1. Análisis de comportamiento general en el escenario 2 71
3.2.2. Análisis de comportamiento según la presencia de los dispositivos 73
3.2.3. Análisis de la presencia según patrones de presencia 74
3.2.4. Análisis de comportamiento según el movimiento de los dispositivos 76
3.2.5. Análisis de tráfico cursado por las redes 77
4. CONCLUSIONES Y FUTURAS LÍNEAS DE TRABAJO 80
4.1. Conclusiones 80
4.2. Futuras líneas de trabajo 81
A. ANEXOS 83
A.1. PRESUPUESTOS 83
A.2. PLANIFICACIÓN TEMPORAL 84
A.3. IMPACTO SOCIAL Y APLICACIONES 86
BIBLIOGRAFÍA 87

Índice de figuras

Figura 1: Para 2021, el 63% del total del tráfico móvil será descargado. 15
Figura 2: Estrategia global para los puntos de acceso WiFi. 15
Figura 3: Estrategia global para puntos de acceso públicos. 16
Figura 4: Tráfico IP según el acceso. 16
Figura 5: Interfaz Fing. 20
Figura 6: Diagrama Nagios. 21
Figura 7: Comparativa Nagios, Zabix, Pandorafms. 22
Figura 8: Screenshot Kismet. 23
Figura 9: Screenshot inssider. 24
Figura 10: Captura Airodump-ng. 25
Figura 11: Una única caja, con 3 puntos de acceso. 30
Figura 12: Distribución de canales. 31
Figura 13: Distribución de la red 802.11 de esta oficina. 31
Figura 14: El Zen de Python. Tim Peters. 35
Figura 15: Raspberry PI3. 36
Figura 16: Antena TP-LINK TL-WN722N. 37
Figura 17: Intercambio de mensajes en protocolo ARP 39
Figura 18: Imagen del paquete ARP. 39
Figura 19: Ejemplo de una hora monitorizando solo con ARP. 40
Figura 20: Trama 802.11. 42
Figura 21: Diagrama flujo fase captura. 44
Figura 22: Diagrama de flujo del funcionamiento del programa principal. 50
Figura 23: Clase Punto de Acceso. 52
Figura 24: Clase Dispositivos. 53
Figura 25: Diagrama de flujo de módulo AP_STA_HANDLING. 55
Figura 26: Tabla que contiene los puntos de acceso. 56
Figura 27: Tabla Dispositivos. 56
Figura 28: Tabla de comportamiento de los dispositivos. 58
Figura 29: Tabla de comportamiento de los puntos de acceso. 58
Figura 30: Diagrama de flujo del módulo Intervalo_Handling. 59
Figura 31: Diagrama de flujo del módulo Data_Handling. 60
Figura 32: Resultado con Airodump-ng. 62
Figura 33: Resultado con sniffer. DB SQlite3 AP1. 62
Figura 34: Gráfica que representa el número de usuarios conectados a la Red Laptops según la marca del dispositivo utilizado para la conexión. 65
Figura 35: Gráfica que representa el número de usuarios conectados a la Red Internet según la marca del dispositivo utilizado para la conexión. 65
Figura 36: Gráfica que representa la presencia de los dispositivos en la Red Laptops durante una semana de lunes a domingo. 66
Figura 37: Gráfica que representa la presencia de los dispositivos en la Red Internet durante una semana, de lunes a domingo. 66

Figura 38: Gráfica que representa la presencia de los dispositivos en la Red Laptops durante una semana y los días divididos en intervalos de 2 horas. 66
Figura 39: Gráfica que representa la presencia de los dispositivos en la Red Internet durante una semana y los días divididos en intervalos de 2 horas. 67
Figura 40: Gráfica de comportamiento de los dispositivos durante un día en la Red Laptops.... 67
Figura 41: Gráfica de comportamiento de los dispositivos durante un día en la Red Internet. ... 67
Figura 42: Número de tramas de DATA y su tamaño cursadas en la red Laptop en una semana. 68
Figura 43: Número de tramas de DATA y su tamaño cursadas en la red Internet en una semana. 69
Figura 44: Gráfica con la cantidad de tramas cursadas por los puntos de acceso en la Red Internet durante una semana de lunes a domingo..... 69
Figura 45: Gráfica con la cantidad de tramas cursadas por los puntos de acceso en la Red Laptops durante una semana de lunes a domingo. 70
Figura 46: puntos de acceso detectados..... 71
Figura 47: Gráfico con porcentaje de dispositivos detectados en la red Internet según su marca. 72
Figura 48: Gráfico con porcentaje de dispositivos detectados en la red Laptops según su marca. 73
Figura 49: Gráfica que muestra la presencia de los usuarios por días en la red Laptops. 73
Figura 50: Gráfica que muestra la presencia de los usuarios por días en la red Internet..... 74
Figura 51: Patrón de presencia 17. 74
Figura 52: Comportamiento de los dispositivos según el movimiento en la red Internet..... 77
Figura 53: Comportamiento de los dispositivos según el movimiento en la red Laptop..... 77
Figura 54: Gráfica con la cantidad y tipo de tráfico cursado en la red Laptop..... 78
Figura 55: Gráfica con la cantidad y tipo de tráfico cursado en la red Internet..... 78
Figura 56: Gráfica que ilustra los presupuestos de los materiales. 83
Figura 57: Gráfica que ilustra los presupuestos de la plantilla. 84
Figura 58: Presupuesto total 84
Figura 59: Diagrama planificación temporal. 85

Índice de tablas

Tabla 1: Diferencia precio Ethernet WLAN. 14
Tabla 2: Estructuración puntos de acceso. 30
Tabla 3: Tabla de las características del Laptop. 32
Tabla 4: Características de Raspberry PI3. 36
Tabla 5: Características técnicas de la antena y foto de la antena. 38
Tabla 6: Campos direcciones según sentido. 47
Tabla 7: Direcciones multicast. 60
Tabla 8: Características escenario 1. 64
Tabla 9: Tipo de tráfico según su longitud. 68
Tabla 10: Características escenario 2. 70
Tabla 11: donde se observa el número y fabricante de los dispositivos utilizados por los usuarios en la Red Internet. 72
Tabla 12: Número y fabricante de los dispositivos utilizados por los usuarios en la Red Laptops. 73
Tabla 13: Patrón de presencia 17 desglosado en días. 75
Tabla 14: Patrón de presencia total. 75
Tabla 15: Presupuestos de los materiales. 83
Tabla 16: Presupuestos de la plantilla. 84
Tabla 17: Planificación temporal. 85

Resumen

Este proyecto se pretende hacer una monitorización y análisis de redes inalámbricas 802.11, con el objetivo de obtener información sobre el estado de la red y de comportamiento de los usuarios. En primer lugar, se implementa un software para realizar la monitorización. Después de decidir el entorno en cual se llevará a cabo la monitorización, se seleccionará el dispositivo que realizará dicha monitorización.

El dispositivo trabajará en modo pasivo capturando todos los paquetes a su alcance, analizará las tramas capturadas seleccionando la información relevante para el estudio, esta información será almacenada en una base de datos para su posterior análisis.

Para su entendimiento, se puede dividir el proyecto en 4 fases:

- Fase de Inmersión: En esta fase se hizo un ejercicio de investigación de las herramientas que escanean redes inalámbricas, posteriormente se realizó un estudio del estándar 802.11, del lenguaje de programación Python y tratamiento de bases de datos. [1]

- Fase de desarrollo: Donde se desarrolló un sniffer propio en el lenguaje Python para la monitorización, análisis, y almacenamiento del tráfico cursado en las redes monitorizadas.

- Fase de monitorización: Una vez preparado el equipo para la monitorización se dejó monitorizando en una planta de oficinas. Se realizó una primera monitorización de un mes y posteriormente una segunda de aproximadamente un mes.

- Fase de análisis: Tras haber realizado la monitorización y tener todos los datos almacenados en una base de datos se procedió al tratamiento y manejo de estos datos para su análisis. En el análisis se pudieron observar mediante gráficas el comportamiento de la red monitorizadas y de sus usuarios.

CAPÍTULO I

1.INTRODUCCIÓN

1.1. Contexto y motivación

En la actualidad el sector de las telecomunicaciones es uno de los más importantes para un país ya que contribuye al desarrollo económico y social, además de facilitar la calidad de vida de las personas.

A través de los años los sistemas de telecomunicaciones se están convirtiendo en imprescindibles tanto para las personas como para el manejo básico de negocios, las empresas están obligadas a pensar en una implantación de tecnologías que se adapten a sus necesidades. Con la globalización las telecomunicaciones han cambiado el estilo de vida la sociedad, también en el ámbito empresarial, de la educación, hospitales, hostelería, etc. El creciente uso de tabletas, teléfonos inteligentes y demás dispositivos inalámbricos permiten a los usuarios estar conectados en cualquier momento y lugar. Esta necesidad de conexión potencia el crecimiento de las redes inalámbricas.

Las redes inalámbricas presentan ventajas como la movilidad, que además del simple hecho de poder conectarse desde cualquier parte de una residencia privada, en el ámbito empresarial puede traducirse en aumento de la productividad de la misma, debido a que cualquiera que tenga acceso a la red puede conectarse a ella desde cualquier lugar dentro del margen de cobertura de la red de forma simple y poder hacer uso de ella en reuniones, diferentes salas, para acceder a información necesaria en cualquier lugar, además los visitantes pueden hacer uso de la red wifi fácilmente, etc. En lugares como hoteles, hospitales, universidades o eventos puntuales, esta sencillez a la hora instalar y de conectar nuevos usuarios puede ser muy útil.

Debido a que no se necesitan cables para su instalación esta será más sencilla y rápida, además en ciertas ocasiones puede ser obligada la necesidad de no usar cables para la instalación de internet, por ejemplo, en edificios históricos, en lugares demasiado amplios donde el cableado es inviable.

Se puede decir también que las redes inalámbricas ofrecen gran flexibilidad en el despliegue, permite libertad de movimiento en la infraestructura, conectar un gran número de dispositivos inalámbricos fácilmente sin necesidad de cables, lo cual lo haría mucho más complejo de realizarse. Permite poder realizar infraestructuras mixtas, es decir, con redes cableadas e inalámbricas para complementar las necesidades. Son flexibles especialmente en cuanto a facilidad para modificación y expansión.

La compatibilidad con los dispositivos inalámbricos es total, la Wi-Fi Alliance asegura la compatibilidad con cualquier dispositivo con la marca Wi-Fi.

El coste de instalar una red wifi es más económico que el de una red cableada, ya que no se necesitan cables ni gran cantidad de conexiones. En ésta tabla obtenida de un artículo en Internet se puede observar la diferencia de instalación de una red sencilla. [2]

	Ethernet	**WLAN**
Puerto Ethernet/PoE	$35	$35
Instalación	$200	$250
Punto de acceso (AP)	-	$1,300 (50 usuarios)
Controlador	-	$15,000 (50 APs)
Costo de instalación para 100 usuarios	$23,500	$16,585
Costo de instalación para 1,000 usuarios	$235,000	$46,700

Tabla 1: Diferencia precio Ethernet WLAN.

Estas características de las redes inalámbricas junto con la actual tendencia de aumento de dispositivos móviles y con ello aumento de tráfico de datos móviles de forma global hace que la tecnología WIFI sea clave en el entorno actual.

El uso de las redes Wi-Fi es omnipresente, según ABI Research, en 2020 se llegará a 41.000 millones de dispositivos conectados a las redes inalámbricas. Según la WBA, asociación líder en la industria del Wi-Fi, en el último año más del 85% de las empresas ha aumentado el nivel de prioridad del Internet of Things (IoT). El Wi-Fi será clave para la conectividad IoT. [3]

Según un informe de Cisco, en 2021 habrá en el mundo más teléfonos móviles (5.500 millones) que cuentas bancarias (5.400 millones), suministros de agua corriente (5.300 millones) o líneas de telefonía fija (2.900 millones). Este informe advierte que se multiplicarán por 7 el tráfico de datos móviles en los próximos 5 años(2016-2021), debido al crecimiento exponencial de usuarios móviles. Las previsiones de Cisco, desvelan que para 2021: [4]

- El tráfico global de datos móviles representará el 20 por ciento del tráfico IP total. En España, el tráfico de datos móviles alcanzará los 4,5 Exabytes anuales o 378 Petabytes mensuales en 2021 (tasa de incremento interanual del 47%). Los 587 Exabytes anuales equivalen a: 122 veces más que todo el tráfico global de datos móviles generado hace 10 años (en 2011); 131 billones de imágenes (como MMS o Instagram).
- Habrá 1,5 dispositivos móviles por persona.
- El número total de smart phones (incluyendo phablets) superará el 50 por ciento del total de dispositivos y conexiones móviles.

La descarga de contenido permite mover datos de una red a otra, una parte considerable del tráfico generada por dispositivos móviles se descarga de la red móvil a la red fija, para este tipo de casos toma especial relevancia las redes WiFi. Para los propósitos del estudio llevado a cabo por Cisco, la descarga pertenece al tráfico generado por dispositivos de modo dual, es decir, dispositivos que soportan conectividad celular y

WiFi. Las predicciones siguientes están basadas tanto en tráfico cursado por puntos de acceso públicos como redes residenciales WiFi. [5]

Como un porcentaje de total de datos móviles generados por todos los dispositivos móviles, la descarga aumentará de un 60%(10.7exabytes/mes) en 2016 al 63% (83.6 exabytes/mes) en 2021. Este volumen de descarga está marcado por la penetración del Smartphone de modo dual y por un porcentaje de uso de Internet móvil en el hogar, empresas, hospitales, empresas, lugares de ocio, etc, tanto con smartphones, como tablets, laptops y cualquier tipo de dispositivo móvil.

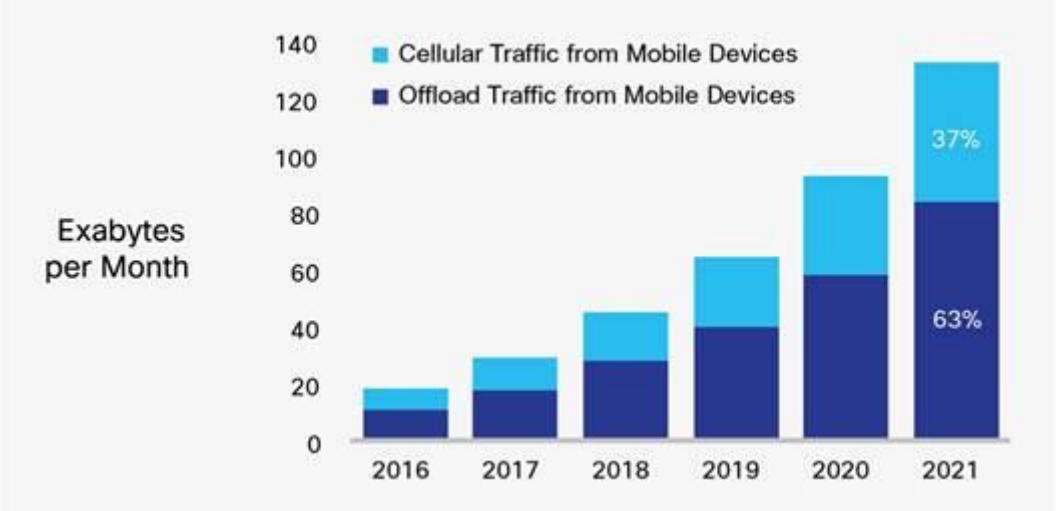


Figura 1: Para 2021, el 63% del total del tráfico móvil será descargado.

Fuente: Cisco VNI Mobile, 2017

Globalmente, crecerá 6 veces el número de puntos de acceso públicos, de 94 millones en 2016 a 541 para el 2021. Los puntos de acceso privados también experimentarán un aumento, de 85 millones en 2016 a 562 millones para 2021.

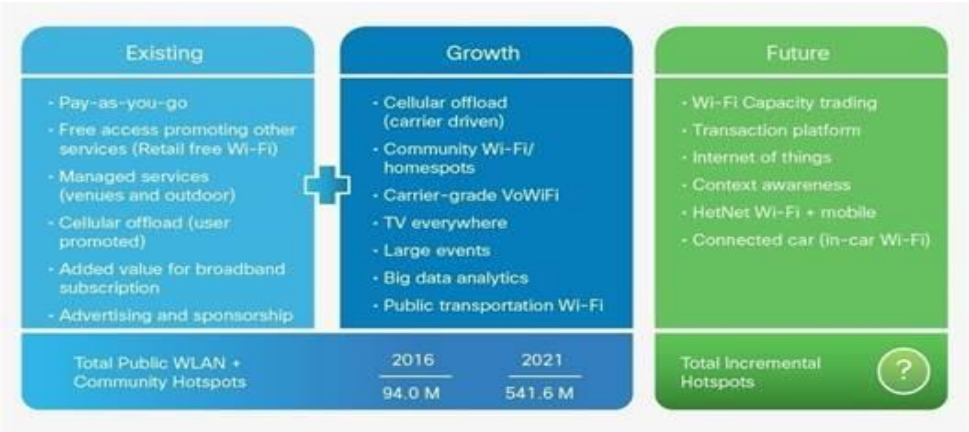


Figura 2: Estrategia global para los puntos de acceso WiFi.

Fuente: Maravedis, Cisco VNI Mobile, 2017.

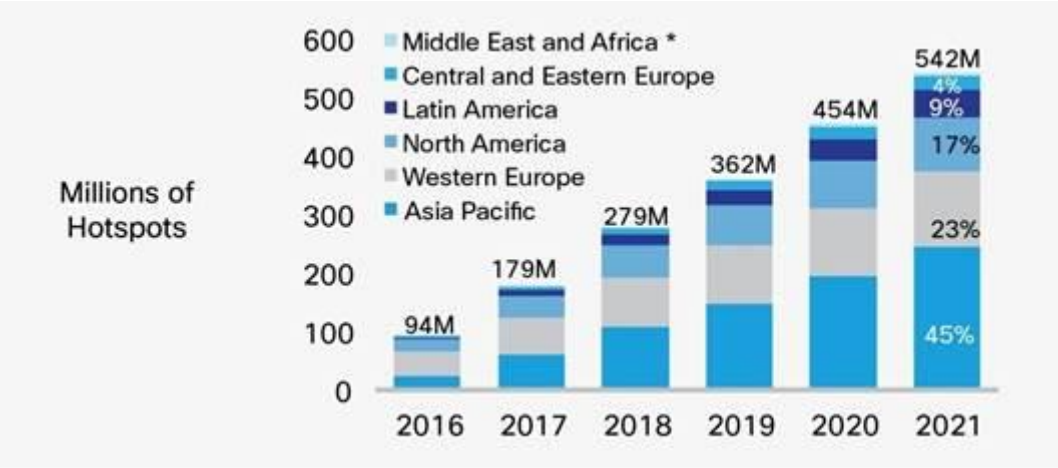


Figura 3: Estrategia global para puntos de acceso públicos.

Fuente: Maravedis, Cisco VNI Mobile, 2017

El acceso WiFi ha sido ampliamente aceptado por los operadores multinacionales a nivel global, y esto lo ha convertido en una red complementaria para propósitos de descarga de tráfico. Esto mismo está ocurriendo con VoWiFi, está evolucionando como un suplemento de la voz celular, extendiendo la cobertura de las redes celulares a través de WiFi.

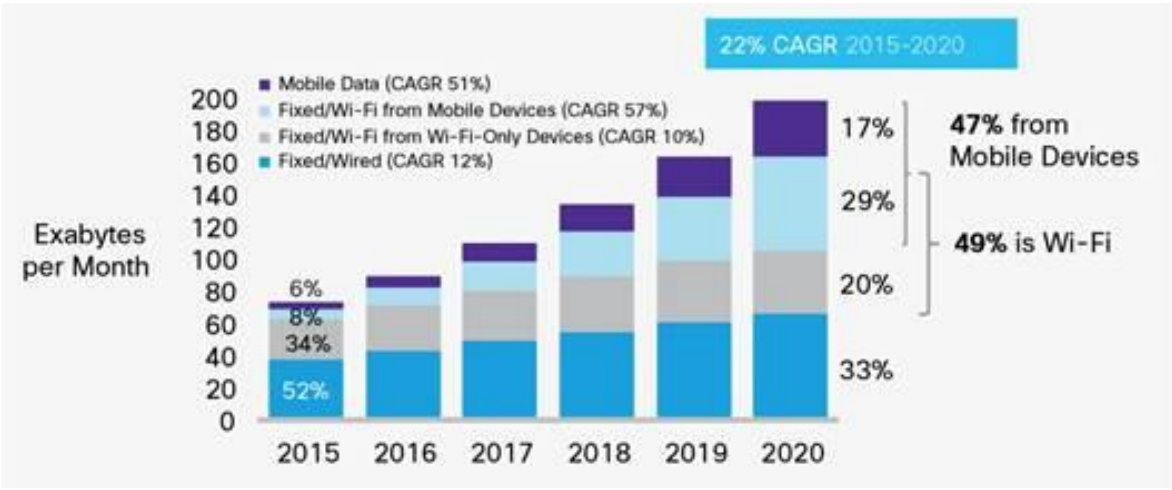


Figura 4: Tráfico IP según el acceso.

Fuente: Cisco VNI Mobile, 2017.

Debido a toda esta evolución, crecimiento e implantación en la sociedad es importante que existan métodos de supervisión análisis y resolución de problemas que puedan ocurrir en las redes inalámbricas. En entornos en los que la seguridad es un elemento esencial, la auditoria de sistemas inalámbricos se convierte en aspecto indispensable.

A pesar de que la Wi-Fi Alliance ha dessarrollado un robusto sistema de cifrado como WPA2, su dispersión espacial no está limitada a un área sino que se expande y es accesible desde cualquier punto de su área de cobertura. Por eso es conveniente reforzar

esta seguridad con herramientas que proporcionen una visión global de la red y ayuden a reforzar la seguridad lo máximo posible.

Sabemos que capturar información sobre 802.11 no conlleva altos costes, simplemente activando el modo monitor de las tarjetas de red para capturar paquetes y un equipo de características aceptables y un software de captura se puede conseguir. Esto puede ser una amenaza o se puede usar de forma preventiva, ya que una monitorización de la red puede aportar beneficios como:

- Optimizar la instalación y componentes de la misma. Se podría conocer los componentes de la instalación y saber cuándo se necesita más hardware o menos.
- Se pueden detectar más fácilmente problemas en el tráfico de la red, cómo por ejemplo, cuellos de botella y saber el causante para así poder solucionar el problema.
- Mediante la información del estado de la red se pueden anticipar problemas y evitar su expansión antes de que se produzcan.
- Se puede detectar tráfico intruso o malintencionado o elementos de la red maliciosos como puntos de acceso falsos, mediante los cuales un usuario podría desvelar datos privados a la hora de conectarse a la red.
- Se pueden aprovechar las características del monitoreo para analizar el comportamiento de la red y mejorar su arquitectura o realizar actualizaciones.
- Tener constancia de vulnerabilidades de la infraestructura que puedan permitir perder el control de la misma o puedan provocar indisponibilidad en el servicio.

Los sistemas de análisis de red son siempre importantes, esta importancia es aún más patente en redes inalámbricas, ya que tienen características adicionales que hacen posible que el riesgo sea mayor. Además, monitorear las redes Wi-Fi es interesante ya que estas permiten varios servicios de valor añadido, como marketing de proximidad, localización de intrusos, análisis de datos, etc. Por todo esto, se ha creído interesante el estudio de comportamiento de una red inalámbrica mediante una herramienta de captura de información de tramas 802.11.

1.2. Marco Regulador

Las redes WLAN cumplen los estándares aplicables a las redes cableadas (IEEE 802.3), además, tienen una norma específica que define el uso y el acceso del espectro radioeléctrico, el primer estándar WLAN fue el IEEE 802.11.

Desde ese momento, la estandarización de las redes WLAN ha sido llevada por varios organismos internacionales, destaca el organismo IEEE con sus estándares 802.11 y sus variantes además del organismo ETSI.

Los dispositivos inalámbricos tienen que cumplir algunas normas y estándares para su uso, debe existir una interoperabilidad entre ellos sin necesidad que sean del mismo fabricante. Estos equipos tienen que seguir normas reguladoras sobre su operación, estas normas deben ser aprobadas según las regulaciones de cada país. [6]

Estas normas reguladoras pueden ser referidas al uso del espectro de radio, protección de datos, impacto ambiental, etc.

A continuación, se van a nombrar otras de las organizaciones certificadoras y reguladoras relacionadas con las redes inalámbricas: [7]

- Wi-Fi Alliance (Wi-Fi). Es una asociación internacional sin fines de lucro. Su principal función es certificar la interoperabilidad de dispositivos WLAN basados en la especificación IEEE 802.11.
- Wireless LAN Association (WLANA). Es una asociación comercial educativa sin ánimo de lucro, su función es ofrecer información sobre temas relacionados con las redes inalámbricas. Además, tiene programas de certificación como CWNA.
- Underwriters Laboratories Inc. (UL). Organización sin ánimo de lucro para la certificación y prueba de los dispositivos basándose en su seguridad.
- La UIT, que tiene una importante presencia en la normalización para el funcionamiento de las redes de TIC.
- Conferencia Europea de Administraciones Postales y Telecomunicaciones (CEPT). Organismo internacional de gestión del espectro.
- Asociación Española de Normalización (AENOR).
- Cuadro Nacional de Atribución de Frecuencias (CNAF).

En España, el Ministerio de Educación y Ciencia es el que se encarga de las comunicaciones inalámbricas, según la Ley 32/2003 General de Telecomunicaciones. En concreto, el órgano superior que se encarga de las comunicaciones radioeléctricas es la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI).

1.2.1. Estándar de IEEE 802.11

Para este proyecto, ya que está centrado en Wi-Fi, interesa la regulación basada en el estándar IEEE 802.11. Las principales funciones del estándar: [8]

- Describe las funciones y servicios que debe implementar un dispositivo para poder operar en una red 802.11.
- Permitir la superposición de diferentes redes 802.11 en un mismo lugar.
- Desarrollo de procedimientos de autenticación y cifrado de las comunicaciones.

El estándar ha ido evolucionando desde su creación con diferentes enmiendas.

1.2.2. Resoluciones de la CMT relacionadas con WIFI/Gestión del espectro

La Ley General de Telecomunicaciones atribuye a la Comisión del Mercado de las Telecomunicaciones (CMT) el establecimiento y supervisión de las obligaciones de los operadores, fomento de la competencia de los mercados, resolución de conflictos entre operadores y ejercer de mediador en ellos [9]. Para el despliegue y explotación de una

red pública de telecomunicaciones, de acuerdo con el artículo 6.2 de la Ley General de las Telecomunicaciones se establece que se requerirá antes del inicio de la actividad la notificación de dicha actividad a la CMT, con los datos de la persona física o jurídica que tenga intención de llevar a cabo la actividad, y la forma en que se va a desarrollar la actividad. En cambio, no se necesitará ninguna notificación previa a la CMT si se trata de una red interna de ordenadores, servidores y diferentes dispositivos de una empresa.

Por tanto, solo se necesitará notificación a la CMT en caso de que se vaya a prestar un servicio o comercializarlo.

Por otra parte, si una compañía desea realizar el despliegue de una red wifi pública deberá hacerlo de acuerdo a la legislación aplicable (Real Decreto 1066/2001 y Orden CTE/23/2002), según el cual deben realizarse cálculos de los niveles de emisiones radioeléctricas que generen las estaciones que formen el sistema y estas medidas deben ser de acuerdo a la O.M. CTE/23/2002.

1.2.3. Ley de protección de datos

Además de las regulaciones en materia de radiación, es necesaria una regulación para proteger la privacidad de los usuarios. La información es una poderosa herramienta, las organizaciones utilizan datos para desarrollar su actividad ya que muchas empresas requieren de datos para conseguir sus propósitos, o en el área publicitaria para identificar posibles clientes según su comportamiento.

En las redes que conectan usuarios a internet los usuarios pueden dejar rastros de datos personales de forma sencilla y sin haberse percatado, esto lleva a generar preocupación en los usuarios, para poder regular el tratamiento de este tipo de datos conflictivos. Para manejar esta situación, en España existe la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, (LOPD) [10], el objeto de esta ley se dispone en el artículo 1 de la misma: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo concerniente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar".*

Este tema cada vez adquiere más importancia en la sociedad actual. Recientemente se ha publicado un anteproyecto de la nueva Ley Orgánica de Protección de Datos, en la que se pretenden añadir algunos cambios.

Existe un reglamento a nivel europeo en lo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, RGPD.

1.3. Productos similares

A la hora de decidir realizar un Trabajo Fin de Grado relacionado con la monitorización de redes inalámbricas, se hizo un estudio de las herramientas disponibles en el mercado. En primer lugar, con herramientas más enfocadas a la capa IP, destacando Fing, y herramientas similares como Net Analyzer, IP Tools, etc.

Fing es una herramienta que permite hacer un escaneo mediante un barrido ping a un determinado rango de direcciones IP, de esta manera se puede saber los dispositivos conectados a una red, obtener datos de su tarjeta de red o conocer los servicios disponibles en estos dispositivos. Tiene una interfaz sencilla y es gratuita.

Figura 5: Interfaz Fing.

Investigando más profundamente acerca de las diferentes herramientas disponibles para el monitoreo y análisis de redes se conocieron herramientas más completas, que hacen un análisis general de red inalámbrica, hardware, servicios de red (SMTP, POP3, HTTP, SNMP...), monitorización de recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), posibilidad de monitorización remota a través de túneles SSL o SSH. Estas herramientas son las que me han parecido más interesantes y han servido de motivación para realizar el proyecto debido a las posibilidades que ofrecen, especialmente para solventar la problemática de la necesidad de auditoria de las redes inalámbricas mencionado en el punto 13.

De este tipo de herramienta se puede destacar:

- **Nagios**

Fue la primera herramienta de este estilo, debido a ello tiene gran penetración en el mercado. Su función es monitorizar el estado de servicios y equipos de una red. Tiene posibilidad de monitorización remota, por ejemplo, comprobar el correcto estado de un servidor, comprobar que un determinado servicio está corriendo de forma adecuada en una máquina específica, etc.

Es una herramienta que proporciona gran versatilidad para consultar casi cualquier parámetro de un sistema. Además, notifica en caso de que detecte algún fallo en algún parámetro del sistema, estos avisos pueden ser recibidos por las personas apropiadas mediante correos electrónicos o mensajes SMS.

Su funcionamiento se puede resumir en la siguiente figura.

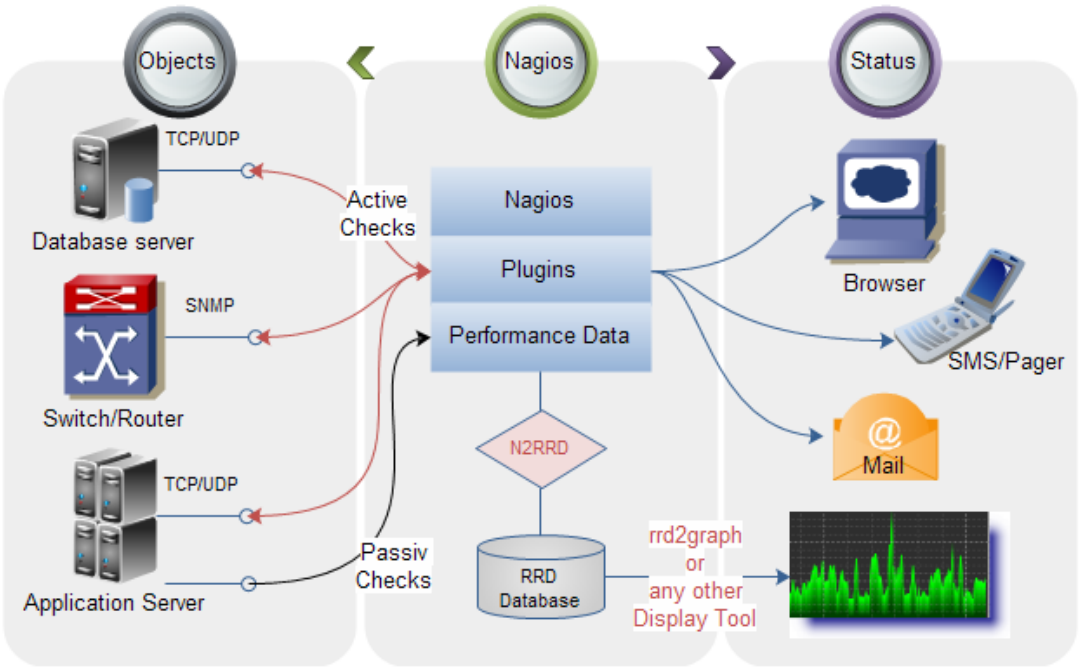


Figura 6: Diagrama Nagios.

- **Zabbix**

Es una herramienta similar a Nagios, es decir, su función es monitorear la capacidad, rendimiento y disponibilidad de los parámetros de una red, también genera avisos mediante SMS o email. Tiene una potente interfaz gráfica y está más orientado a la visualización de gráficas.

Por el contrario que Nagios, utiliza templates para las monitorizaciones.

Según un estudio realizado por la compañía Pandorafms su principal desventaja es que aunque se ha usado en grandes instalaciones, a partir de 1000 nodos puede disminuir su rendimiento. [11]

- **Pandorafms**

Es menos conocida que las dos anteriores, la funcionalidad es similar a estas dos anteriores, monitorización de red, servidores, aplicaciones y generación de alertas e informes. Está enfocada totalmente al ámbito empresarial, tiene versión libre y de pago. La versión libre puede monitorizar 10000 nodos sin reducción de rendimiento. Cuenta con funcionalidades completas de integraciones con terceros vía API.

También cabe mencionar su integración con dispositivos móviles gracias a su sistema de geolocalización.

Con estas tres herramientas se puede realizar un análisis completo de la red, detección de problemas, prevención de problemas, predicción de mejoras, análisis de datos, etc.

Con esta comparativa, realizada por la compañía Pandorafms, podemos ver las características de cada una. [11]

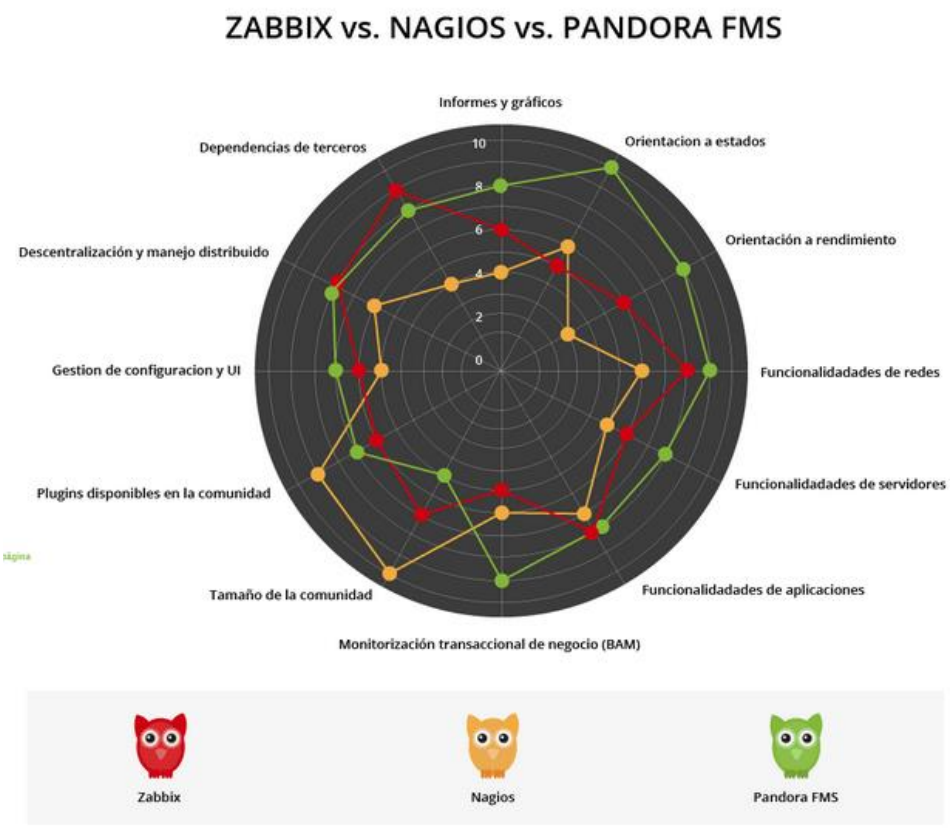


Figura 7: Comparativa Nagios, Zabix, Pandorafms.

Las siguientes herramientas son menos completas que las anteriores pero se asemejan más a la solución proporcionada en este proyecto, además de resultar muy interesantes, han servido de gran ayuda a la hora de elegir que cabeceras de las tramas 802.11

capturadas eran más interesantes de almacenar y con las que había más posibilidades de realizar un estudio más completo.

- **Kismet**

Kismet es un detector de redes inalámbricas, sniffer, y sistema de detección de intrusos. Trabaja principalmente con redes Wi-Fi, pero puede manejar otros tipos de redes mediante plugins. Funciona con cualquier adapatador wireless que soporte el modo de monitorización raw, puede husmear tráfico 802.11 a/b/g/n.

Una diferencia que se puede apreciar con respecto a otros sniffers es su funcionamiento pasivo, captura los paquetes de la red sin generar tráfico en dicha red, permite la detección de puntos de acceso y dispositivos asociando unos con otros. Kismet adicionalmente tiene nociones básicas de sistemas de detección de intrusos, asi como detección de ciertos ataques a redes inalámbricas.

El funcionamiento a grandes rasgos de Kismet se podría resumir en captura de paquetes, envío de estas capturas a un servidor que analizará los datos y los organizará, interpretará y publicará, finalmente los usuarios de esta herramienta podrán observar estos datos recogidos por el servidor.

Por otro lado, en comparación con el programa sniffer desarrollado en este proyecto, el funcionamiento de captura de paquetes en modo pasivo es muy similar, nuestro programa también funciona en modo pasivo, sin generar tráfico en las redes que monitoriza y es capaz de detectar puntos de acceso y dispositivos, estos ultimos gracias a la asociación a los puntos de acceso, tal y como lo hace Kismet.

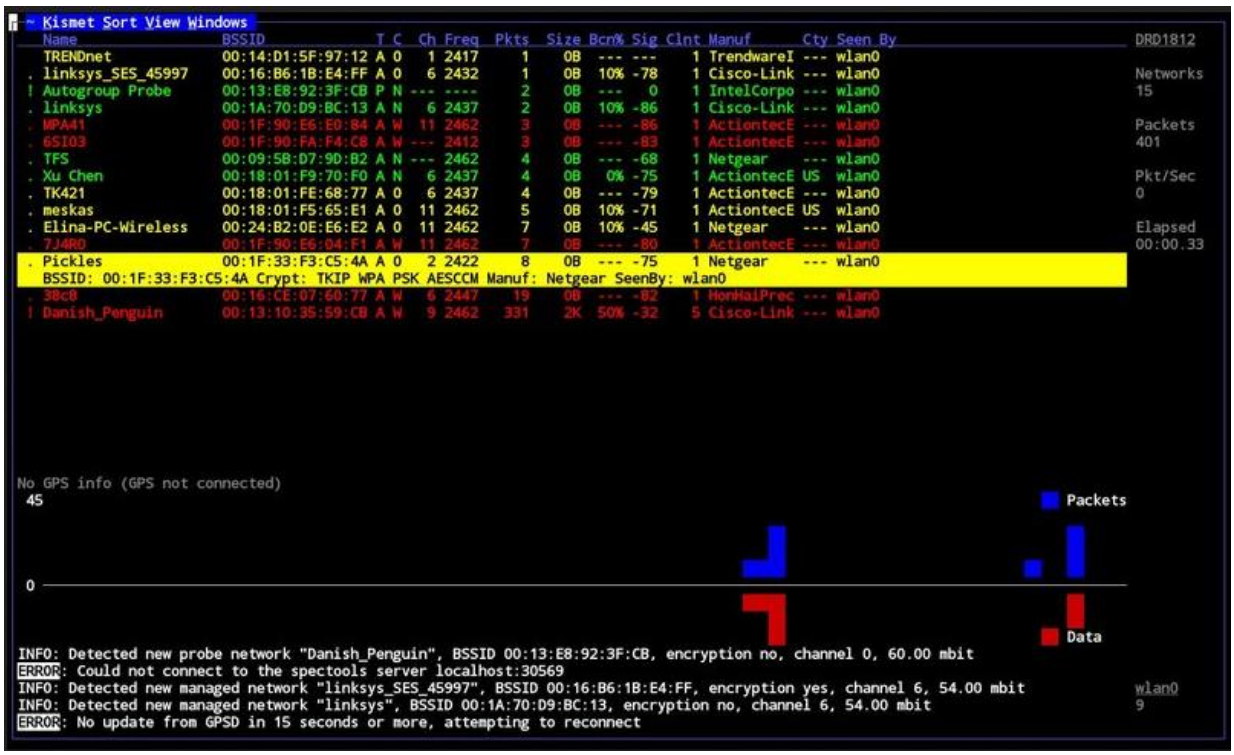


Figura 8: Screenshot Kismet.

- **inSSIDer**

Esta aplicación resulta interesante incluirla debido a que analiza las tramas 802.11 y obtiene información diferente al resto de analizadores vistos hasta el momento, ha sido útil en cuanto a inspiración de que cabeceras capturar y que análisis se pueden realizar posteriormente.

Es una aplicación que detecta redes inalámbricas al alcance del equipo donde se esté ejecutando y muestra gráficamente la intensidad de sus señales. La aplicación escanea muchísimos puntos de acceso cercanos a nuestro equipo. Se puede obtener gran cantidad de información como vemos en la siguiente imagen.

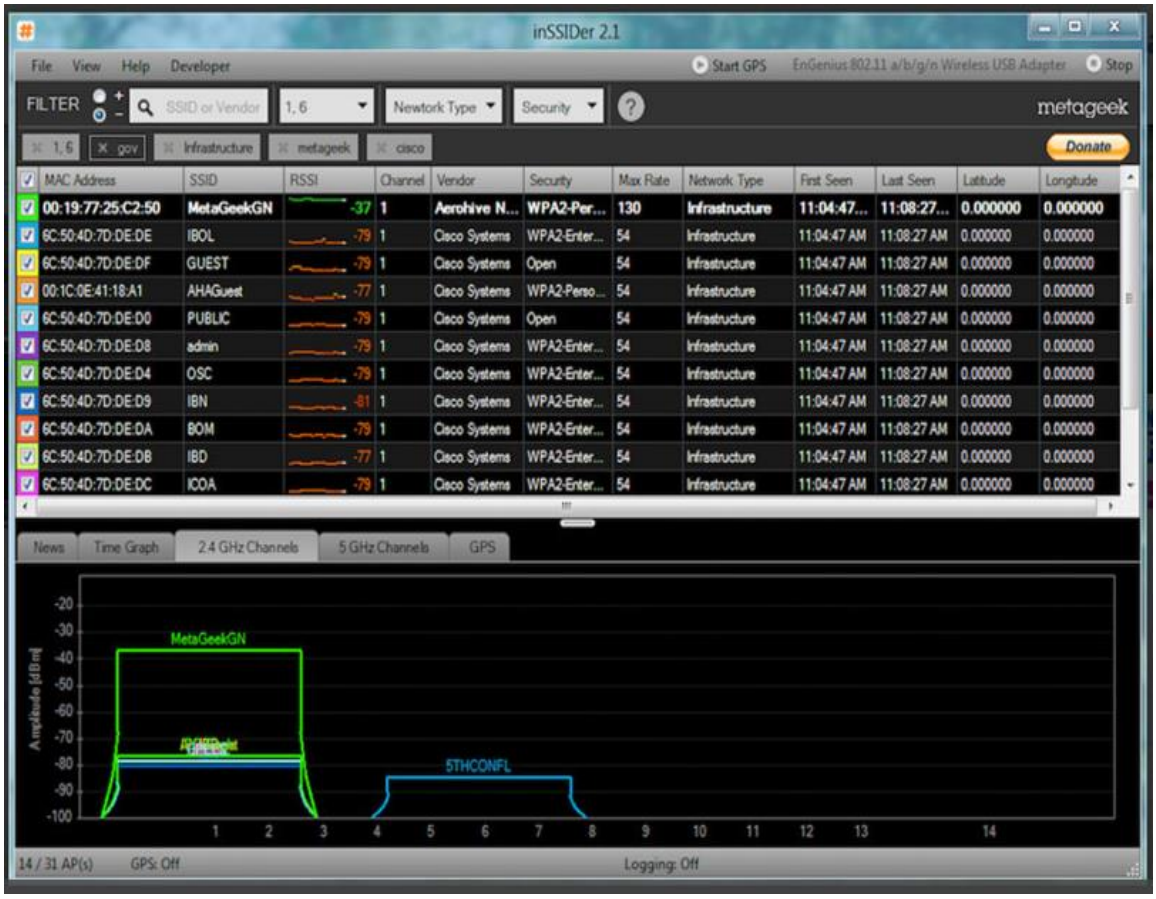


Figura 9: Screenshot inssider.

Se pueden mencionar muchas otras herramientas similares como Netstumbler, ntopng, etc.

Finalmente, se va a comentar brevemente algunas de las herramientas que más parecido tienen con el programa desarrollado en este proyecto. Más parecido en cuanto a que se centran principalmente en la captura, son sniffers, únicamente capturan tramas, no realizan tareas de almacenamiento y análisis. Sin embargo, si proporcionan los datos para que el usuario haga con ellos lo que estime oportuno.

Estas herramientas podrían reemplazar a nuestro programa sniffer, es decir, se podría haber ustilizado cualquiera de estas tres herramientas mencionadas para conseguir los datos, almacenarlos en la base de datos y finalmente haber hecho el análisis sobre esos datos obtenidos gracias a estas herramientas. En lugar de eso, se ha desarrollado un programa sniffer que cumplirá esta función.

- CommView

Es un sniffer de redes 802.11 a/b/g/n, consigue una descripción detallada y fácil de entender. Soporta más de 70 protocolos, destaca también el manejo de decifrado de paquetes de datos codificados con claves WEP o WPA. Adicionalmente posee un módulo VoIP para un análisis de SIP y H.323.

- Airodump-ng

Pertenece a la suit Aircrack-ng, Airodump-ng es usado para la captura de paquetes en modo pasivo. Adicionalmente, si se tiene un recptor GPS conectado al equipo donde se ejecute Airodump, este será capaz de reconocer las coordenadas de los puntos de acceso detectados.

Debido a la similitud con el objetivo que se pretendía que cumpliese el programa de la solución de este proyecto. Esta herramienta ha sido utilizada en este proyecto para realizar comprobaciones, se ha ejecutado simultáneamente con el programa desarrollado para corroborar que el funcionamiento del programa implementado ha sido el correcto

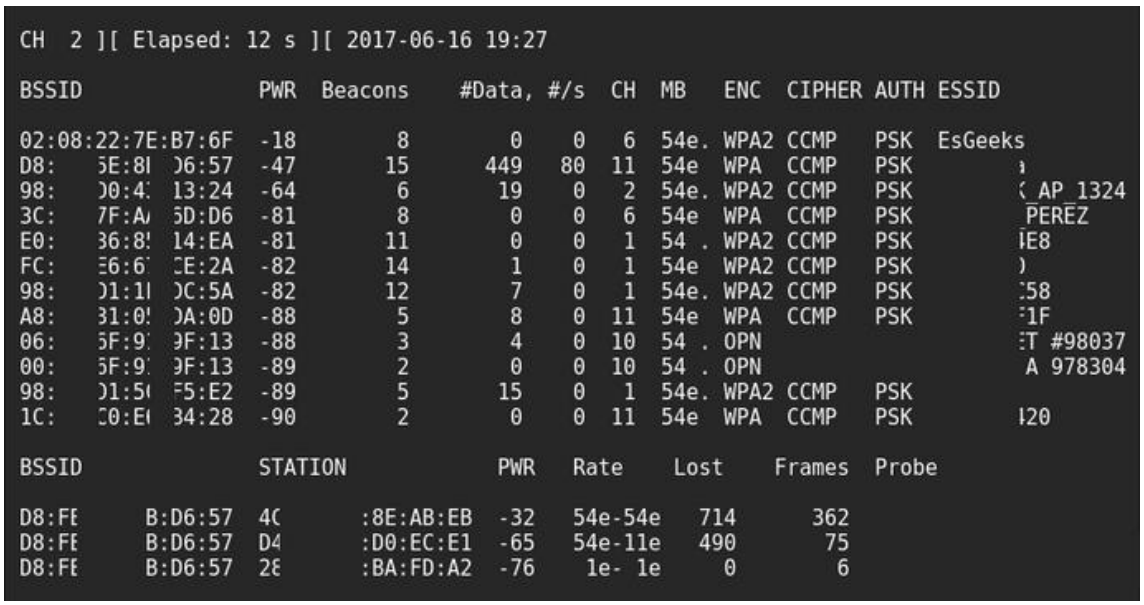


Figura 10: Captura Airodump-ng.

Hay otras muchas herramientas que pueden ser utilizadas como sniffers, entre ellas mencionar Tcpdump, muy similar a Airodump.

Estas herramientas podrían reemplazar a nuestro programa sniffer, es decir, se podría haber utilizado cualquiera de estas tres herramientas mencionadas para capturar las

tramas 802.11, almacenarlas en la base de datos y finalmente haber hecho el análisis sobre esos datos obtenidos gracias a estas herramientas. En lugar de eso, el proyecto se ha centrado en gran medida en el desarrollo de dicho programa.

1.4. Objetivos

Este Trabajo Fin de Grado tiene como objetivo la monitorización y análisis del tráfico en una red inalámbrica IEEE 802.11, para ello se pretende desarrollar un sistema que permita capturar el tráfico de la red.

El sistema está formado por:

- Un programa desarrollado por el alumno, que se podría equiparar a un sniffer de redes inalámbricas trabajando en modo pasivo, ejecutándose en un equipo Raspberry. El propósito de este programa es la de detectar y capturar tramas 802.11.
- Una base de datos en la que se almacenarán dichas tramas.
- Un proceso de tratamiento y organización de los datos almacenados.
- Un proceso de análisis de los resultados obtenidos.

El objetivo específico de este programa será capturar las cabeceras de las tramas, las cuales contendrán información relevante para el análisis, y almacenar dicha información en una base de datos para su posterior análisis basado en el comportamiento de los dispositivos a nivel de tipo de tráfico, presencia en la red, etc.

Los principales objetivos marcados y conseguidos hasta su finalización han sido los siguientes:

- Estudio del estándar IEEE 802.11.
- Estudio de herramientas de escaneo de redes, como Fing, Net Analyzer, Netscan, Acrylic, Wireshark, Airodump, Tcpdump, etc.
- Consideraciones y elección del tipo de monitorización.
- Preparación de equipo y estudio del lenguaje de programación Python [11].
- Desarrollo y validación del programa desarrollado en Python.
- Captura y monitorización de tráfico.
- Almacenamiento de datos en una base datos.
- Tratamiento y manejo de estos datos.
- Análisis de los resultados.

CAPÍTULO II

2.DESARROLLO DE LA SOLUCIÓN

En este capítulo se va a explicar cómo se ha desarrollado la solución y su correspondiente justificación.

2.1. Diseño del sistema

2.1.1. Descripción

El sistema está formado por:

- Un programa desarrollado por el alumno, que se podría equiparar a un sniffer de redes inalámbricas trabajando en modo pasivo, ejecutándose en un equipo Raspberry. El propósito de este programa es la de detectar y capturar tramas 802.11.
- Una base de datos en la que se almacenarán dichas tramas.
- Un proceso de tratamiento y organización de los datos almacenados.
- Un proceso de análisis de los resultados obtenidos

Existe una amplia gama de herramienta profesionales desarrolladas para monitorizar las redes tanto en modo activo como pasivo. Son herramientas ampliamente usadas y fiables.

Para este proyecto se decidió crear una herramienta desarrollada en lenguaje Python, que permitiese al alumno desarrollar sus conocimientos en dicho lenguaje de programación, y a su vez, trabajar a bajo nivel las tramas de 802.11, donde la herramienta Wireshark ha resultado de mucha ayuda a la hora de monitorizar, ya que permite comparar y ver claramente de donde viene la información que busca a nivel de byte. [13]

El objetivo principal del programa es la monitorización de una planta de oficinas donde los usuarios están en su mayoría conectados a la red wifi, tanto en su laptop como en los dispositivos móviles tradicionales (smartphones, tablet, etc,). Se pretende monitorizar la actividad de los usuarios de dicha oficina tanto desde punto de vista de su comportamiento a nivel de tráfico, así como a nivel presencial. Para poder analizar toda la información monitorizada esta se almacenará en una base de datos.

La función del programa es ejecutarse en un equipo con su tarjeta de red en modo pasivo, de tal forma que le permitirá estar escuchando en varias redes a la vez y además no será necesario autenticarse en las redes para poder monitorizarlas. Todas las tramas detectadas al alcance del equipo serán analizadas gracias al programa y la información relevante será almacenada en una base de datos si cumplen los requisitos que previamente hemos especificado en el programa.

En resumen, con esta solución se pretende monitorizar una red wifi para el estudio de comportamiento de los usuarios y de la propia red, para posteriormente analizarlos y poder sacar diferentes conclusiones, podemos dividir la solución en:

- Captura
- Análisis (automático) de la trama capturada
- Almacenamiento de la información relevante en una base de datos.
- Tratamiento y manejo de los datos almacenados.
- Análisis final.

2.1.2. Escenario

En este apartado se explicará donde se ha realizado la monitorización y las características más relevantes de dicho entorno.

El escenario elegido para llevar a cabo el estudio ha sido una oficina de trabajo, un entorno que cumplía los requisitos necesarios para las necesidades el proyecto.

Es una oficina en la que los usuarios se conectan a la red mediante dispositivos inalámbricos como smartphones, tablets, laptops, etc. Además, se realiza teletrabajo por lo que podremos observar variación en la actividad de la red. Para saber dónde estaban

Dicha oficina está equipada con 80 puestos de trabajos, de los cuales el 75% de ellos son puestos asignados para teletrabajo, con lo que el número total de usuarios es indeterminado desde punto de vista que son fluctuantes por el uso del teletrabajo, así como que la oficina contiene dos plantas más de usuarios, que visitan la planta la cual estamos monitorizando

Se ha realizado una monitorización de un mes, del 29 de mayo al 3 de julio, debido a que se ha realizado una monitorización pasiva se han detectado 3 redes, las cuales se han monitorizado al mismo tiempo ya que no ha hecho falta conectarse a ninguna de ellas.

Por motivo de privacidad de la información, cambiaremos las direcciones MAC’s encontradas por nombres anónimos. Esto significa:

Redes WIFI: SSID-1, SSID-2, …, SSID-n

Puntos de Accesos: BSSID-1, BSSID-2, …, BSSID-n

Dispositivos: STA1, STA2, STA3, …, STAn

A las redes detectadas las llamaremos:

- *Red 1: Laptops*
  Esta es la red interna corporativa, a ella se conectan los empleados con sus laptops corporativos, necesitan de una autorización para ser identificados como empleados de la empresa.
- *Red 2: Internet*
  Es una red también corporativa en la que se conectan principalmente los smartphones personales de los empleados.
- *Red 3: Guest*
  Es la red destinada para invitados, es decir, personas externas a la empresa que acuden a ella de forma puntual, no necesita autentificación y es la que menos carga de tráfico tiene.

Durante la monitorización se han detectado 9 puntos de acceso(AP), 3 puntos de acceso por cada red, cada uno de los tres puntos de acceso operando en un canal diferente, concretamente en el canal 1, 6 y 11, por tanto, el entorno está diseñado de manera que no se produzcan solapamientos. Los puntos de acceso en la oficina según el canal por el que transmiten: [13]

Red	Transmitiendo ch11	Transmitiendo ch1	Transmitiendo ch6
Red Internet	BSSID-1	BSSID-4	BSSID-7
Red Guest	BSSID-2	BSSID-5	BSSID-8
Red Laptop	BSSID-3	BSSID-6	BSSID9

Tabla 2: Estructuración puntos de acceso.

Figura 11: Una única caja, con 3 puntos de acceso.

En esta figura se ilustra cómo es una única caja, en la oficina donde se ha realizado la monitorización había 3 de ellas. Los puntos de acceso que contiene tienen una distribución de canales adecuada para no solaparse, es decir, un punto de acceso transmite por el canal 1, otro por el canal 6 y otro por el canal 11.

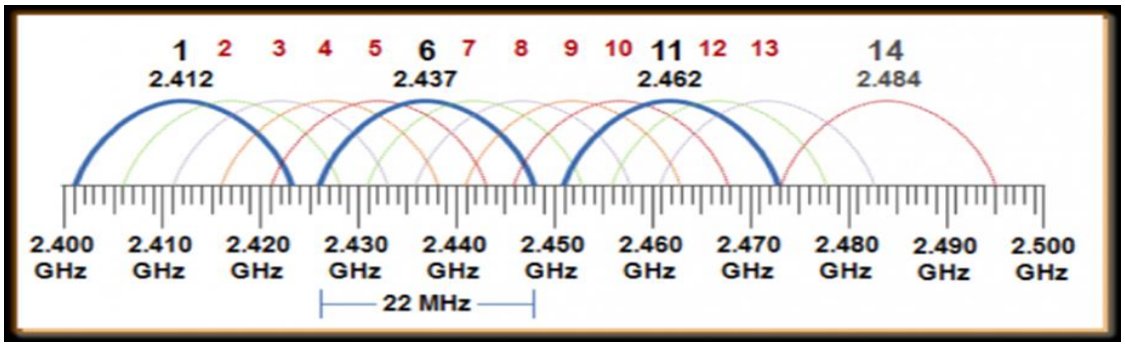


Figura 12: Distribución de canales.

Cómo se puede apreciar en la figura, solo pueden solaparse los APs que se encuentran localizados en una misma caja, debido a ello los APs que se encuentran en una misma caja tienen una distribución de canales por los que transmiten adecuada para que no se produzcan solapamientos, es decir, canales1, 6 y 11. Ya que las cajas están situadas a distancia suficiente entre ellas como para que no interfieran sus señales, los puntos de acceso de cajas diferentes si pueden transmitir en el mismo canal. [22]

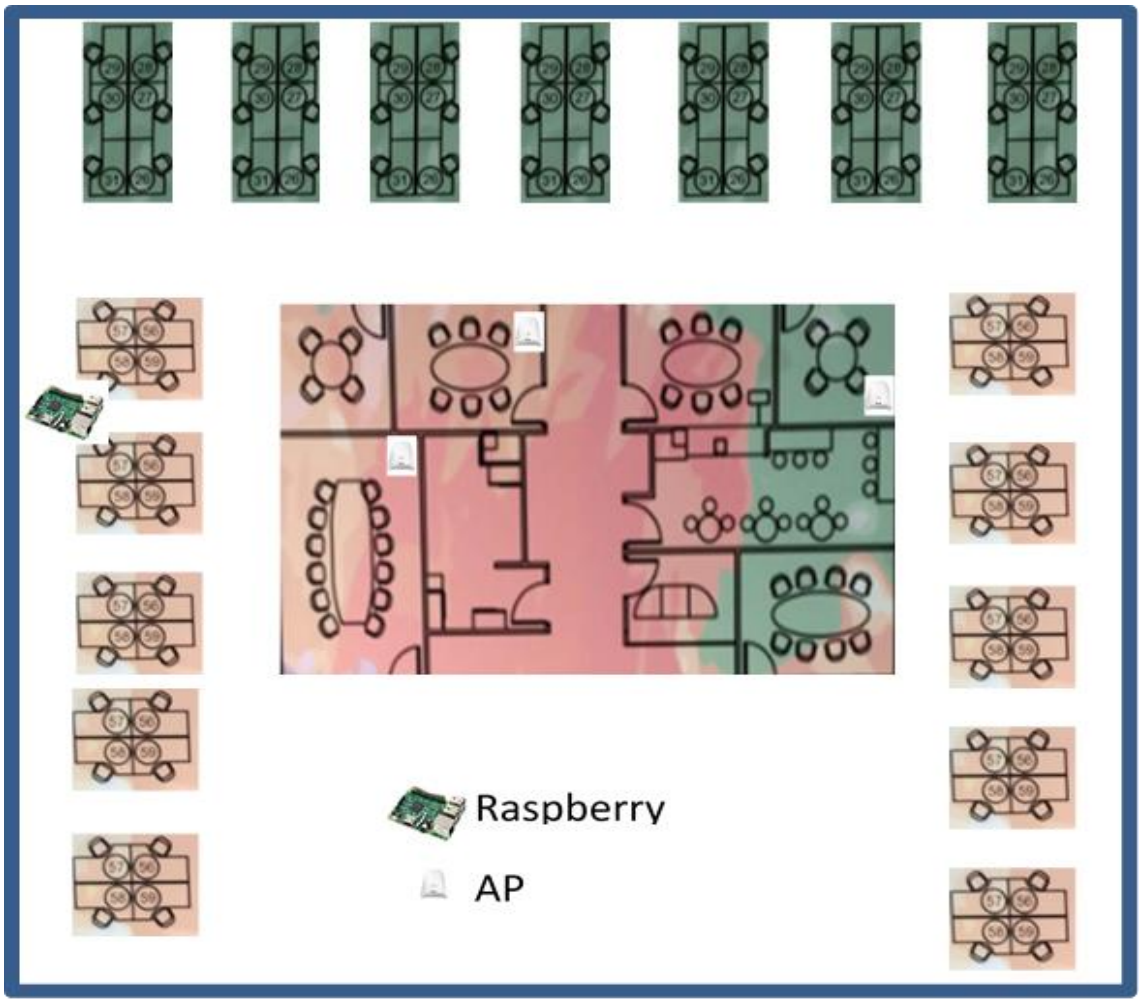


Figura 13: Distribución de la red 802.11 de esta oficina.

2.1.3. Componentes del sistema

En este apartado van a describir las características de los equipos y softwares utilizados para desarrollar el proyecto.

El sistema consta de 5 partes fundamentales:

- Raspberry PI3, conectada a la red de forma pasiva.
- Sniffer desarrollado en Python, será ejecutado en la raspberry
- Base de datos SQLite3, almacenada en una tarjeta SD en la raspberry.
- Consultas, se realizarán consultas durante el monitoreo.
- Análisis, se analizarán gráficamente los resultados obtenidos.

Para implementar este sistema se han utilizado diferentes dispositivos, los cuales han funcionado con su tarjeta de red en modo monitor.

- ***Ordenador portátil***

  Como premisa inicial se necesitaba un equipo con una tarjeta de red capaz de capturar paquetes en modo monitor. La implementación del programa en Python requería de un equipo que permitiera desarrollar el programa de forma cómoda, con teclado y pantalla.
  Además, era necesaria cierta potencia en el procesado para poder ejecutar el programa, al menos un equipo con características técnicas medias, ya que el programa captura un gran número de tramas en periodos de tiempo muy corto e ininterrumpidamente. Por otra parte, para comprobar que dicho programa estaba funcionando correctamente se han usado herramientas profesionales, que requieren de un procesador igualmente de al menos de características medias, como Airodump-ng corriendo en dicho equipo.

  Las características técnicas de este equipo las podemos ver en la siguiente tabla:

Nombre	ASUS X555LJ
RAM	8GB
Tarjeta de Red	Qualcomm Atheros AR956x QCWB335
Estandares soportados	IEEE 802.11 b/g/n
SO	Ubuntu 16.04.3 LTS 64 bits
Procesador	Intel Core i7-5500U
CPU	2,4 GHz
Tarjeta Grafica	NVIDIA GeForce 920M
Encriptacion	WEP, WPA. WPA2 (AES, TKIP)

Tabla 3: Tabla de las características del Laptop.

Como se puede observar en la tabla, como sistema operativo se ha elegido Ubuntu 16.04.3, la principal razón por la cual se ha elegido desarrollar el programa en esta distribución es debido a la posterior compatibilidad con el sistema operativo cargado en la Raspberry, ya que en primera instancia el programa sería implementado en este equipo laptop y posteriormente se ejecutaría en la Raspberry, a la cual se le deberá instalar un software libre, gratuito. Desde el primer momento se sabía que podía ser interesante utilizar una o varias Raspberries, o dispositivos similares, para realizar la monitorización, por tanto, se decidió que Ubuntu 16.04.3 [14], al ser un software libre basado en GNU/Linux era una buena opción. Está orientado al usuario medio, con enfoque a la sencillez en su manejo, está compuesto de diverso software generalmente distribuido bajo licencia libre. De esta forma, se reducirían costes.

La mayoría de los elementos de un equipo laptop como puede ser el procesador, la memoria RAM, discos duros, tarjeta gráfica, etc se aprovechan mejor usando Linux ya que el consumo de recursos es menor que en Windows.
Además, las distribuciones GNU/Linux suelen tener gran estabilidad de sistema, esta característica es clave para un programa sniffer en continua ejecución, en cuanto a la seguridad, la probabilidad de que se produzcan infecciones es remota, los creadores de virus rara vez atacan a software Linux (debido principalmente a su baja cuota de mercado).

Seguramente debido a esta estabilidad y seguridad, la distribución GNU/Linux es ampliamente escogido por desarrolladores de código, por tanto, existe infinidad de información técnica para poder solventar casi cualquier problema, tanto técnico como a nivel de programación. Esto resulta muy interesante a nivel académico para poder continuar aprendiendo sobre entornos GNU/Linux.

A la hora de instalar softwares, debido a que normalmente la paquetería de software de Ubuntu está actualizada, se puede asegurar que se está instalando la última versión compatible lo cual siempre genera mayor confianza. Además, de forma específica había algunos softwares que entre sus características estaba la de mejor funcionamiento en Linux que en Windows.

Los softwares principales utilizados en este equipo han sido los siguientes:

- **Aircrack-ng** [15]

Es una suite de software de seguridad inalámbrica. Está formada por un analizador de paquetes, un crackeador de redes WEP y WPA/WPA2-PSK y otro amplio conjunto de herramientas para auditoria inalámbrica.

Las más utilizadas son:

- Aircrack-ng: Descifra la clave de los vectores de inicio
- Airodump-ng: Escanea las redes y captura vectores de inicio
- Aireplay-ng: Inyecta tráfico para elevar la captura de vectores de inicio

- Airmon-ng: Establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores

La suite está implementada para utilizarse con Linux, la versión de Windows también se puede utilizar aunque es de peor calidad.

Esta suite es óptima para tarjetas de red Atheros, como la de este equipo y con algunas Ralink, como la antena adicional instalada en la Raspberry.

En este equipo se ha utilizado Airmon-ng, cuyo cometido ha sido activar el modo monitor de la tarjeta de red para de esta manera poder capturar tramas.

- **Wireshark** [16]

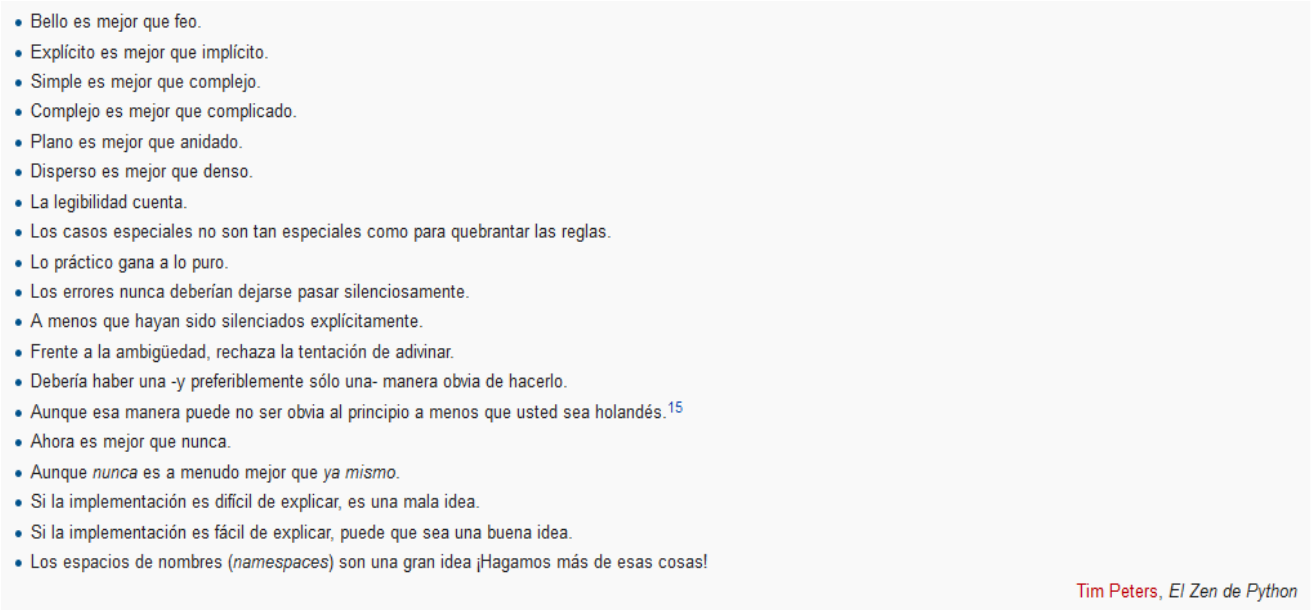
Wireshark es un analizador de protocolos de código libre, tanto para Windows como para Linux. Se utiliza para realizar análisis de redes y solventar problemas, además puede ser utilizado como herramienta didáctica para el estudio de los diferentes protocolos de red, soporta más de 1100. Cuenta con gran cantidad de filtros junto con una interfaz intuitiva enfocada al usuario que permite desglosar por capas cada uno de los paquetes capturados, siendo posible visualizar los campos de cada una de las cabeceras y capas de los paquetes capturados.

Esta funcionalidad de desglose ha sido imprescindible a la hora de desarrollar el programa sniffer, ya que permite sumergirse en la trama y poder conocer al detalle cada uno de los campos de forma relativamente fácil gracias a los numerosos filtros y la claridad de su interfaz, ha resultado ser clave para poder realizar un correcto análisis de las tramas 802.11.

- **Python**[12]

Python es un lenguaje de programación cuyo principal objetivo es una sintaxis que facilite la compresión del código. Es un lenguaje de programación que soporta orientación a objetos, programación imperativa y funcional. Además, es un lenguaje multiplataforma soportado en MAC, Windows y Unix, también máquinas virtuales y .NET, aunque en un principio se desarrolló para Unix. Está preparado para ser utilizado para desarrollar cualquier tipo de programa.

La filosofía de Python está descrita en estos principios escritos por el desarrollador de Python Tim Peters.



- Bello es mejor que feo.
- Explícito es mejor que implícito.
- Simple es mejor que complejo.
- Complejo es mejor que complicado.
- Plano es mejor que anidado.
- Disperso es mejor que denso.
- La legibilidad cuenta.
- Los casos especiales no son tan especiales como para quebrantar las reglas.
- Lo práctico gana a lo puro.
- Los errores nunca deberían dejarse pasar silenciosamente.
- A menos que hayan sido silenciados explícitamente.
- Frente a la ambigüedad, rechaza la tentación de adivinar.
- Debería haber una -y preferiblemente sólo una- manera obvia de hacerlo.
- Aunque esa manera puede no ser obvia al principio a menos que usted sea holandés.[15]
- Ahora es mejor que nunca.
- Aunque *nunca* es a menudo mejor que *ya mismo*.
- Si la implementación es difícil de explicar, es una mala idea.
- Si la implementación es fácil de explicar, puede que sea una buena idea.
- Los espacios de nombres (*namespaces*) son una gran idea ¡Hagamos más de esas cosas!

Tim Peters, *El Zen de Python*

Figura 14: El Zen de Python. Tim Peters.

La versión utilizada ha sido Python 3.5. Se ha elegido este lenguaje de programación debido a que es uno de los más utilizados actualmente, es utilizado por grandes compañías multinacionales como Google, Nokia e IBM. Por ello, se puede decir que uno de los principales motivos ha sido didáctico, es decir, aprender a utilizar este leguaje. Es relativamente sencillo familiarizarse con este lenguaje, está centrado en la legibilidad. Dispone de muchísima información para el desarrollo, existen muchas librerías, tipos de datos, funciones, módulos, etc, que están incorporadas en el propio lenguaje y que se pueden utilizar para realizar nuevos programas. La versatilidad y capacidades son enormes.

Por otro lado, es un lenguaje que al ser orientado a objetos permite que nuestro programa pueda ser reutilizado de forma sencilla. Presenta gran flexibilidad para la extensión pudiéndose incluso escribir módulos en c o c++.

- **SQLite3** [18]

Como base de datos se ha utilizado SQLite, un sistema de gestión de bases de datos. Se ha elegido SQLite debido a que cuenta con librerías para poder utilizarse con Python de forma sencilla simplemente con importar el módulo correspondiente, además las bases de datos creadas con esta librería se almacenan como un solo archivo y como no tiene dependencias es fácilmente portable, lo cual es útil en este proyecto debido a que se tiene que pasar los datos de la Raspberry al pc portátil para realizar el tratamiento de datos y análisis de los mismos.

- ***Raspberry PI3***

Para poder llevar a cabo la monitorización durante un largo periodo de tiempo y en diferentes escenarios se requería de un dispositivo que se pudiese dejar sin ocupar espacio y que pudiese cumplir con los objetivos del proyecto, es decir,

tener capacidad de procesado suficiente para ejecutar el programa desarrollado en Python y capturar tramas en modo pasivo. Además, para almacenar la información capturada debía tener memoria suficiente, para lo cual se tuvo que añadir a este equipo una tarjeta SD de 16 Gb.

Figura 15: Raspberry PI3.

La raspberry PI3 utilizada tiene las siguientes características técnicas:

Nombre	Raspberry PI3
Procesador	Chipset Broadcom BCM2387.
CPU	1,2 GHz de cuatro núcleos ARM Cortex-A53
RAM	1GB LPDDR2
Puertos Ethernet	Ethernet 10/100 BaseT
USB	USB 4 x Conector USB 2.0
Dimensiones	8.5 x 5.3 cm
Antena externa	TP-LINK TL-WN722N
SO	UBUNTU MATE 16:04
Kernel	Linux kernel 4.19.1
Estandares soportados	IEEE 802.11 b/g/n

Tabla 4: Características de Raspberry PI3.

Se ha instalado en la Raspberry como sistema operativo Ubuntu MATE 16:04, es un sistema operativo gratuito con base de Linux Ubuntu. Se ha elegido principalmente para que sea totalmente compatible en todos los sentidos con el programa sniffer desarrollado en Python, es decir, que no hubiera ningún problema a la hora de "entender" el código, ya que según el sistema operativo las sentencias en Python pueden ser diferentes. Al instalar Ubuntu MATE se podrá comprobar que tiene incorporados las siguientes aplicaciones: [16]

- Linux kernel 4.19.1

- MATE 1.12.2
- Firefox 46.0.1
- Thunderbird 38.8.0
- LibreOffice 5.1.2.2
- Shotwell 0.22.0
- Rhytmbox 3.3
- VLC media player 2.2.2
- Scratch
- Minecraft Pi
- Python (2.7 & 3.5)
- IDLE (Integrated Development Environment for Python)
- tilda (F12 drop-down terminal emulator)

Además de estas aplicaciones se han usado otros softwares, dándoles un uso exactamente igual que en laptop, explicado en el punto anterior.

- Wireshark
- Aircrack-ng. Concretamente Airodump-ng y Airmon-ng.

Por último, mencionar qué para poder realizar una correcta monitorización en modo pasivo, se ha tenido que añadir una antena externa a la Raspberry (WLAN de la Raspberry no acepta el modo pasivo), cuyas características se explicarán a continuación.

- ***Antena***

Se necesitaba poner la tarjeta de red de la raspberry en modo monitor, para ello se ha requerido de una antena externa ya que la tarjeta de red por defecto de la raspberry no ofrece esta funcionalidad, la elegida ha sido: TP-LINK TL-WN722N

De esta forma se mejora la calidad de la captura, con esta antena se consigue la mitigación de la perdida de datos y los obstáculos en una oficina.

Figura 16: Antena TP-LINK TL-WN722N.

Nombre	TP-LINK TL-WN722N
Puerto USB	1 x USB 2.0
Botón	Botón WPS
Dimensiones	93.5 x 26 x 11mm
Tipo de antena	Desmontable Omnidireccional (RP-SMA)
Ganancia de la antena	4dBi
Estandares soportados	IEEE 802.11 b/g/n
Tasa de señal	11n: Hasta 150Mbps(dinámica) 11g: Hasta 54Mbps(dinámica) 11b: Hasta 11Mbps(dinámica)
Sensibilidad de recepción	130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Encriptación	WEP, WPA-PSK/WPA2-PSK
Modulación	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Funciones avanzadas	WMM, Roaming

Tabla 5: Características técnicas de la antena y foto de la antena.

2.2. Fundamentos de la solución

En este apartado se va a proceder a explicar algunas consideraciones para el desarrollo de la solución así como las principales características del sistema.

2.2.1. Consideraciones para la monitorización

El propósito principal del proyecto es monitorizar una red IEEE 802.11 para analizar el comportamiento de los dispositivos conectados a ella, tanto a nivel de tráfico como presencial. Este escaneo de la red se puede hacer de diferentes maneras:

- Monitorización activa: Monitorización activa se entiende como el escaneo de la red 802.11 mediante el envío de manera periódica de paquetes request a toda la red, para esperar una contestación por parte de los dispositivos conectados a la misma y de esta forma verificar quien está conectado. Esto se puede hacer mediante el envío de mensajes ARP [19], como se ha visto anteriormente cuando se ha mencionado el programa de escaneo de redes wifi Fing. Como una de las

primeras pruebas que se hicieron a modo de toma de contacto con la solución a desarrollar, ya que fue una de las soluciones valoradas como solución posible, fue precisamente un programa que hacía escaneos periódicos mediante envío de mensajes ARP a un rango de direcciones perteneciente a la red que se pretende escanear, tal y como lo hace la herramienta Fing.

El funcionamiento del protocolo ARP es el siguiente:

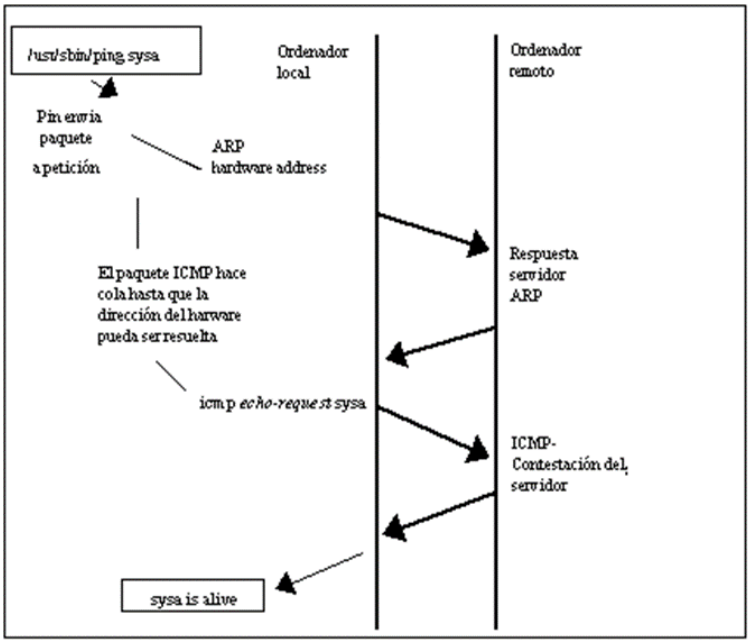


Figura 17: Intercambio de mensajes en protocolo ARP

El principal objetivo del protocolo ARP es averiguar la dirección física de una tarjeta de red de un dispositivo con una determinada dirección IP.

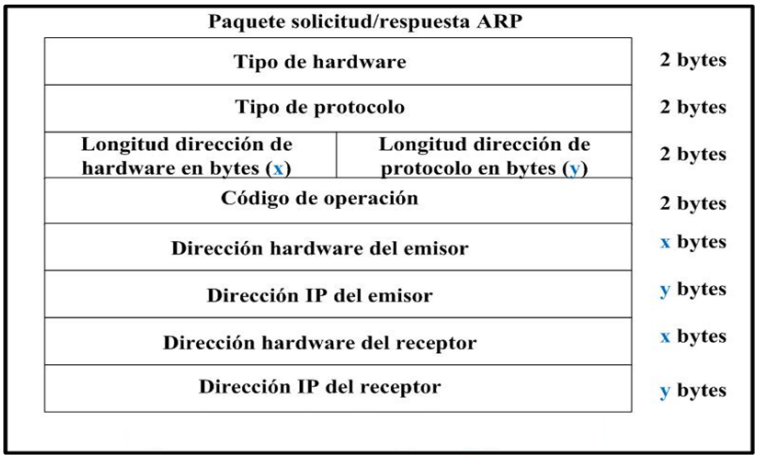


Figura 18: Imagen del paquete ARP.

Mediante estos escaneos periódicos la información obtenida es la dirección física de los dispositivos conectados a la red en cada momento en concreto y la hora, por tanto, haciendo escaneos periódicos podemos saber cómo se ha estado comportando un dispositivo en concreto en periodos de tiempo más largos, una hora, un día, una semana, un mes, etc.

DIA_U	HORA_U	Dest_MAC	Source_MAC	Type	Hardware_type	Protocol_type	Hardware_size	Protocol_size	Opcode	SourceMAC	Source_IP	DestMAC	Dest_IP
Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Fil...	Filtro	Filtro	Filtro	Filtro
07/09/17	16:49:08	b827eb220b41	6c198fbf8768	0806	0001	0800	06	04	0002	6c:19:8f:bf:87:68	192.168.1.37	b827eb220b41	192.168.1.45
07/09/17	16:49:08	b827eb220b41	ec086b1f0249	0806	0001	0800	06	04	0002	ec:08:6b:1f:02:49	192.168.1.41	b827eb220b41	192.168.1.45
07/09/17	16:54:08	b827eb220b41	6c198fbf8768	0806	0001	0800	06	04	0002	6c:19:8f:bf:87:68	192.168.1.37	b827eb220b41	192.168.1.45
07/09/17	16:54:11	b827eb220b41	ec086b1f0249	0806	0001	0800	06	04	0002	ec:08:6b:1f:02:49	192.168.1.41	b827eb220b41	192.168.1.45
07/09/17	16:54:11	b827eb220b41	28be03090469	0806	0001	0800	06	04	0002	28:be:03:09:04:69	192.168.1.33	b827eb220b41	192.168.1.45
07/09/17	16:59:08	b827eb220b41	6c198fbf8768	0806	0001	0800	06	04	0002	6c:19:8f:bf:87:68	192.168.1.37	b827eb220b41	192.168.1.45
07/09/17	16:59:08	b827eb220b41	e05f4511df7b	0806	0001	0800	06	04	0002	e0:5f:45:11:df:7b	192.168.1.34	b827eb220b41	192.168.1.45
07/09/17	16:59:08	b827eb220b41	ec086b1f0249	0806	0001	0800	06	04	0002	ec:08:6b:1f:02:49	192.168.1.41	b827eb220b41	192.168.1.45
07/09/17	16:59:08	b827eb220b41	28be03090469	0806	0001	0800	06	04	0002	28:be:03:09:04:69	192.168.1.33	b827eb220b41	192.168.1.45
07/09/17	16:59:08	b827eb220b41	4c74036ed995	0806	0001	0800	06	04	0002	4c:74:03:6e:d9:95	192.168.1.39	b827eb220b41	192.168.1.45
07/09/17	17:04:08	b827eb220b41	6c198fbf8768	0806	0001	0800	06	04	0002	6c:19:8f:bf:87:68	192.168.1.37	b827eb220b41	192.168.1.45
07/09/17	17:04:08	b827eb220b41	e05f4511df7b	0806	0001	0800	06	04	0002	e0:5f:45:11:df:7b	192.168.1.34	b827eb220b41	192.168.1.45
07/09/17	17:04:08	b827eb220b41	ec086b1f0249	0806	0001	0800	06	04	0002	ec:08:6b:1f:02:49	192.168.1.41	b827eb220b41	192.168.1.45
07/09/17	17:04:08	b827eb220b41	28be03090469	0806	0001	0800	06	04	0002	28:be:03:09:04:69	192.168.1.33	b827eb220b41	192.168.1.45
07/09/17	17:09:08	b827eb220b41	6c198fbf8768	0806	0001	0800	06	04	0002	6c:19:8f:bf:87:68	192.168.1.37	b827eb220b41	192.168.1.45
07/09/17	17:09:08	b827eb220b41	28be03090469	0806	0001	0800	06	04	0002	28:be:03:09:04:69	192.168.1.33	b827eb220b41	192.168.1.45
07/09/17	17:09:08	b827eb220b41	ec086b1f0249	0806	0001	0800	06	04	0002	ec:08:6b:1f:02:49	192.168.1.41	b827eb220b41	192.168.1.45

Figura 19: Ejemplo de una hora monitorizando solo con ARP.

Las ventajas en este TFG de hacer este tipo de monitorización son:

- Menor complejidad en el código de programación.
- Mayor eficacia en los resultados de la monitorización, ya que se va a detectar cualquier dispositivo conectado a la red, este activo o no lo este, es decir, este generando tráfico o no esté generando tráfico.

Las desventajas son:

- Como hemos visto en el funcionamiento de la herramienta Fing, realizaremos peticiones ARP a toda la subred para ver que direcciones ip han sido asignadas y de esta manera averiguar que dispositivos están conectados a la red. Estas peticiones serían enviadas cada 5 o 10 minutos, lo que puede producir una excesiva carga de tráfico en la red y provocar que la red no funcione al 100% debido a la carga enviada y rse reciban quejas por parte del administrador de red del entorno elegido para la monitorización, o incluso cabe la posibilidad de que en algunas redes exista alguna medida de seguridad que al detectar varias ráfagas de peticiones ARP, se bloquea la posibilidad de seguir enviando ráfagas para evitar ataques de inundación de la red.

- Con estas peticiones ARP, obtendremos del rango de direcciones IP de la subred la dirección física de los dispositivos que tengan asignadas dichas direcciones IP, y la hora a la que se recibe las contestaciones por parte de los dispositivos. Por tanto, la única información que se tiene para realizar el estudio es la MAC de los dispositivos conectados a la red y las horas en las que han estado conectados.
- Para realizar las peticiones ARP se necesita estar conectado a la red donde se pretenda realizar el escaneo, por tanto, necesitamos autenticarnos en la red. Esto limita las posibilidades de uso, es decir, solo se podría ejecutar el programa en redes donde tengamos autorización. Además, no podríamos monitorizar varias redes simultáneamente ya que no podemos estar conectados a la vez en varias redes.

- Monitorización pasiva: Mediante monitorización pasiva el dispositivo elegido para la monitorización, con su tarjeta de red en modo pasivo se mantiene escuchando, es decir, capturando las diferentes tramas que cursan la red, tanto las que no se dirigen a él, que normalmente desecharía, como las que van dirigidas a él. Captura todo el tráfico cursado en la red que está escuchando.

  Las ventajas para este TFG son:
  - No se carga la red debido a que no se necesita enviar ningún mensaje de petición.
  - No se necesita autenticarse en la red para monitorizarla. Esto implica que se puede monitorizar varias redes simultáneamente, como es el caso de este proyecto en que se monitorizan 3 redes al mismo tiempo. Además, los entornos en los cuales se podría realizar el proyecto aumentan, debido a que no se necesitaría autenticación para poder monitorizar la red.
    Tenemos acceso a la trama 802.11 completa, es decir, a todos los campos excepto la parte de contenido de datos cifrada, que no podemos saber que contiene. Podemos observar que se puede acceder a los campos relevantes de la trama según la figura 20. Al tener acceso a más información el estudio del posterior análisis puede ser más completo. [13]

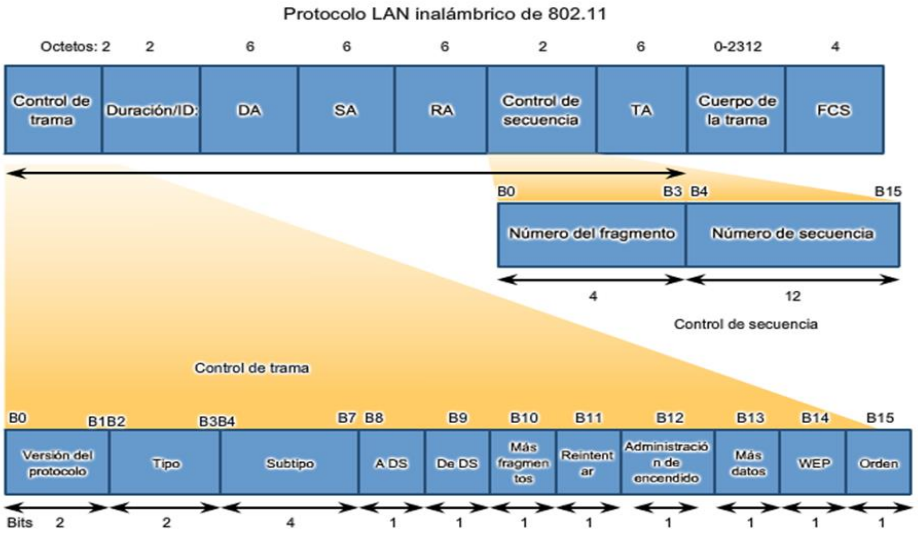


Figura 20: Trama 802.11.

Como desventajas se pueden encontrar:

- Mayor complejidad en el código del programa, ya que hay que analizar más información.
- Mayor complejidad a la hora de identificar dispositivos conectados a la red en el caso de que no estén generando tráfico.

En este proyecto se ha priorizado en la opción de monitorización pasiva, ya que valorando los pros y los contras de cada una para el objetivo marcado se ha considerado más interesante, especialmente la posibilidad de tener acceso a la trama 802.11. Esto ha dado la posibilidad de entender mejor dicha trama, mejorar los conocimientos del estándar y de Python al inspeccionar dicha trama. En definitiva, hacer un estudio de comportamiento más completo.

2.2.2. Características del sistema

- Arranque automático por reinicio. [20]
- Posibilidad de monitorizar una o varias redes simultáneamente
- Gran autonomía de almacenamiento. Debido a la optimización en la captura de información, solamente almacenamos la información relevante para el análisis.
- Análisis de comportamiento en tiempo real por intervalo.

2.3. Implementación de la solución

En este apartado se van a explicar los elementos softwares desarrollados y utilizados para la implementación de la solución.

La implementación de la solución se ha dividido en 2 fases:

- Fase de captura.
- Fase de validación.

2.3.1. Fase de captura

En esta fase se tratará la temática de cómo el programa desarrollado captura y analiza las tramas.

2.3.1.1. Objetivo

La principal tarea que se pretende realizar implementando el programa es un programa que sea capaz de capturar las tramas 802.11, además que sea capaz de inspeccionar dicha trama y extraer los campos relevantes para el estudio. [13]

El programa es el encargado de monitorizar las redes 802.11 y recopilar datos para su posterior análisis. Se usará una única Raspberry, la cual estará preparada para monitorizar, es decir, tendrá su tarjeta de red en modo monitor y el programa ejecutándose.

Según las características del sistema vistas anteriormente se sabe que es posible monitorizar varias redes 802.11 simultáneamente, en este caso se monitorizará el tráfico de tres redes.

El programa arranca automáticamente una vez detectadas las redes, va analizando las tramas y extrayendo información relevante para el estudio, de los puntos de acceso(APs) y los dispositivos(STA), de la trama detectada extrae dicha información siguiendo los patrones previamente establecidos en el código del programa. A la hora de la detección de los puntos de acceso se utiliza un filtro de la potencia de la señal con la que se recibe la trama, de esta manera se evita monitorizar tramas enviadas por puntos de acceso demasiado alejados cuyo tráfico que llega a la Raspberry es bastante espurio y difícil de consolidar. El número de usuarios sin tener este filtro es excesivo debido a que se detectan tramas generadas por puntos de acceso de otras plantas, por ejemplo, de las plantas adyacentes a la planta monitorizada.

La monitorización está basada en un programa desarrollado en Python, su funcionamiento genérico, es capturar tramas en modo pasivo, inspección de dicha trama y extracción de datos relevantes.

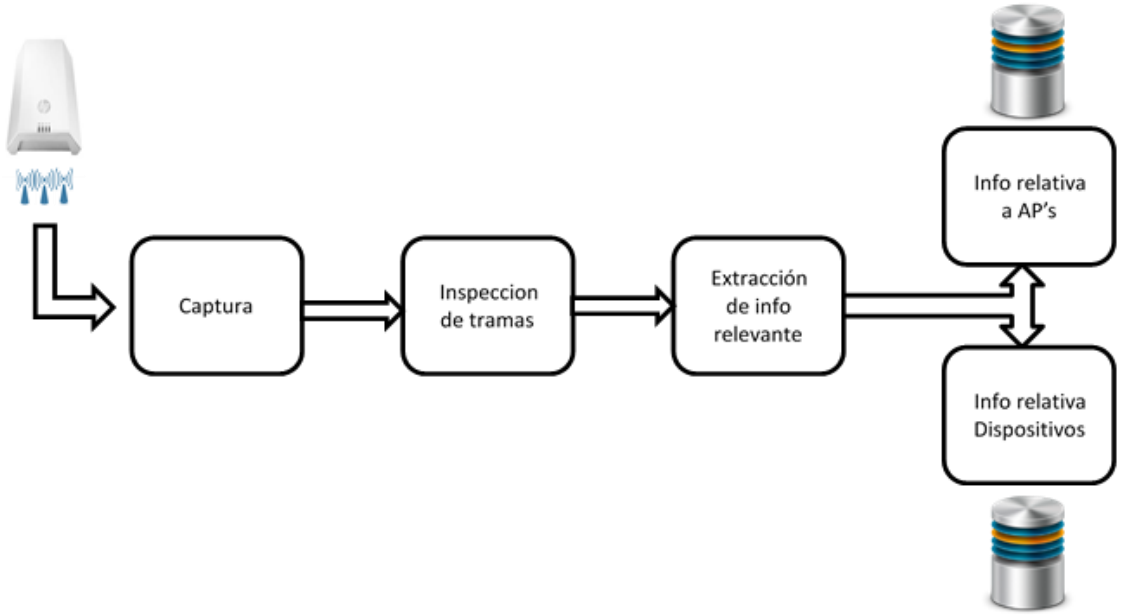


Figura 21: Diagrama flujo fase captura.

Para poner el equipo en modo pasivo utilizamos el software mencionado anteriormente 'Airmon-ng':

Empezar modo monitor: *sudo airmon-ng start nombretrajetared*

Salir de modo monitor: *sudo airmon-ng stop mon0*

2.3.1.2. Datos de entrada a la fase de captura

En la fase de captura hay determinados datos que se pueden modificar en el código del programa antes de comenzar la monitorización, a pesar de que el programa tiene arranque automático, estos datos tienen unos valores por defecto en caso de que no se quieran modificar.

- SSID: Hay que conocer que redes se desea monitorizar, el programa necesita las SSID de dichas redes, como se ha mencionado anteriormente debido a la monitorización en modo pasivo podremos monitorizar varias redes a la vez.
- Ventana de comportamiento: Para optimizar lo máximo posible la monitorización, es decir, perder el menor tiempo posible en procesamiento y volcado de datos a la base de datos, se ha establecido que se harán dichos volcados periódicamente cada cierto tiempo previamente establecido, de esta manera también se conseguirá un análisis automático de comportamiento en base a alguno de los datos recabados lo cual también requiere de cierto tiempo de procesado. Esto se reflejará en que tendremos datos en la base datos escalados en ventanas de ese tiempo que se haya establecido.
  Esta ventana temporal se puede elegir y variar de acuerdo a las siguientes consideraciones:

1. Tamaño de la red/redes que se vayan a monitorizar. Hay que tener en cuenta que el análisis del comportamiento se hace el tiempo real, si la ventana fuera pequeña, y el número de dispositivos en la red grande, no daría tiempo a hacer el análisis del comportamiento.
2. Si la ventana temporal es demasiado pequeña, debido a la gran cantidad de datos que tendría que procesar cargaría mucho el procesador y además no añadiría información útil, por ejemplo, el estado de un dispositivo a las 12:00 va a ser muy similar al estado del dispositivo a las 12:01. El objetivo del estudio es observar el comportamiento durante un plazo largo de tiempo, es decir, horas, días, semanas y meses.

Para este proyecto, teniendo en cuenta estas premisas, se ha considerado que una ventana de una hora era razonable para cubrir los objetivos del estudio, de esta forma se podrá realizar un estudio del comportamiento de los dispositivos durante horas, días, semanas y meses.

Además, se podría combinar monitorización pasiva con monitorización activa, como se ha visto en puntos anteriores la activa se realizaría mediante el envío de ráfagas de mensajes ARP, teniendo en cuenta las limitaciones de este tipo de tráfico, aunque esta funcionalidad no se ha incluido en este proyecto.

2.3.1.3. Captura de la información

El programa sigue unas premisas en concreto a la hora de analizar las tramas que detecta, es decir, no captura una trama y directamente la guarda, hace un análisis automatizado de las tramas que captura y solo guarda los datos relevantes según las premisas que se le hayan dado en el código. Esto hace que en la base de datos se almacenen solo los datos relevantes para el estudio, lo cual facilitará mucho a la hora de realizar el análisis como se podrá observar en el punto de *Análisis* de esta memoria. Los pasos que sigue el programa a la hora de capturar la información son los siguientes:

- DETECCIÓN DE LOS APS Y DISPOSITIVOS CONECTADOS A ELLOS

Debido a que el equipo, en este caso una Raspberry, está en modo monitor capturará las tramas que detecte. El programa se encarga de inspeccionar cada trama que llega y decidir si debe ser analizada y que campos analizar.
Para inspeccionar la trama de forma adecuada ha sido necesario conocer de forma teórica los campos de la trama 802.11, teniendo en cuenta que no siempre es el mismo orden, dependerá del tipo de trama 802.11. Gracias al estudio del estándar IEEE 802.11 se ha podido almacenar en variables dentro del programa todos los tipos de tramas que existen en este protocolo, de manera que el programa podrá conocer el tipo de trama que está tratando. También ha sido de gran ayuda la herramienta Wireshark, con la cual se puede observar claramente en qué posición de la trama está cada campo.

El programa captura las tramas una a una, lo primero que analiza de la trama capturada es el campo tipo de trama: Se buscan los tipos BEACON y PROBE RESPONSE con ellas se detectará si estas tramas recibidas pertenecen a las redes que se desean monitorizar leyendo el campo de SSID, si son de estas redes se obtiene la MAC Address del AP. Con estas tramas se consiguen los puntos de acceso que están conectados a las redes que se pretenden monitorizar, por tanto, guardamos la información relativa al punto de acceso en una tabla de la base de datos SQLITE3 utilizada, en esta tabla tendremos los puntos de acceso que tiene dicha red junto con información relevante obtenida de las tramas en las que aparecieran.
Entonces, tenemos una TABLA de puntos de acceso(AP), contendrá todos los puntos de acceso conectados a la red/redes monitorizadas. A esta tabla se accede cada vez que se detecta un punto de acceso que no se hubiese visto en periodos anteriores y que pertenezca a las redes monitorizadas

- Se buscan los tipos de trama DATA, con ellas se detectan los dispositivos que están enviando tramas de datos a través de los puntos de acceso conectados a las redes, detectados anteriormente, con lo que se puede asegurar que son dispositivos conectados a dichas redes.
- Se guardará en una nueva tabla de la base de datos la información obtenida de las tramas relevante a los diferentes dispositivos detectados, esta tabla contendrá entonces todos los dispositivos que han estado conectados a las redes de forma única, es decir, el número de usuarios únicos conectados a las redes, y a que red está conectado cada usuario. A esta tabla se accede cada vez que se detecta en la trama capturada una dirección MAC nueva, es decir, cada vez que se detecta un nuevo usuario.

- INFORMACIÓN DE COMPORTAMIENTO SOBRE LOS APs

Para monitorizar el comportamiento de los APs, se creará una nueva TABLA en la que se almacenarán datos relevantes al comportamiento de los puntos de acceso. Para ello, se va a utilizar la anteriormente mencionada ventana temporal, por tanto, mediante intervalos de tiempo se irá accediendo a la tabla para actualizar los campos que se han considerado relevantes para el estudio, la tabla de comportamiento de los AP, para cada AP detectado, consta de los siguientes campos:

- DIA de detección del AP.
- HORA de detección del AP.
- Red WIFI(SSID) a la que pertenecía el AP.
- Dirección MAC del AP(BSSID).
- Canal por el que está transmitiendo el AP.
- Potencia den dbm con que se recibe la trama.
- Número de tramas Beacon que ha cursado el AP.
- Número de tramas Probe Response que ha cursado el AP.
- Número de tramas de Datos que ha cursado el AP.
- Cantidad de bytes/seg que ha cursado el AP.

Esta información será usada posteriormente para realizar el análisis de los datos recabados sobre el comportamiento de los puntos de acceso conectados a las redes. Esta información se ha almacenado en la tabla de comportamiento de puntos de acceso de forma automatizada facilitando en gran medida su posterior análisis.

- INFORMACIÓN DE COMPORTAMIENTO SOBRE LOS DISPOSITIVOS

A la hora de monitorizar el comportamiento de los dispositivos conectados a las redes que se pretenden monitorizar se creará también una nueva TABLA, y se utilizará la misma ventana temporal anterior para actualizar esta tabla. Se actualizará, por tanto, al mismo tiempo que la tabla de comportamiento de los puntos de acceso.
Esta tabla se llama tabla de comportamiento de los dispositivos y contiene los siguientes campos por cada registro en la tabla:

- DIA
- HORA, como se actualiza según la ventana temporal, esta hora será el intervalo utilizado.
- Red WIFI(SSID) a la que está conectado el dispositivo.
- Dirección MAC del dispositivo.
- Punto de acceso al que está conectado el dispositivo(BSSID).
- Comportamiento del dispositivo durante el intervalo de tiempo declarado, este análisis se hace de forma automatizada, para declarar el estado se han seguido las siguientes premisas:
    - Conectado: Si el dispositivo ha enviado y recibido tramas de datos durante el intervalo de tiempo.
    - Activo: Si el dispositivo ha enviado tramas de datos pero no las ha recibido.
    - Pasivo: Si el dispositivo ha recibido pero no ha enviado tramas de datos durante el intervalo de tiempo.
    - Ausente: Si el dispositivo no ha enviado ni recibido tramas de datos durante el intervalo de tiempo.

- Dirección en la que viaja la trama de datos, campo importantísimo para poder inspeccionar la trama de forma correcta, ya que dependiendo del valor de este campo la posición de las cuatro direcciones MAC que contiene la trama 802.11 varía. En los campos de direcciones se pueden encontrar RA, TA, SA, BSSID. [20]

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	not used
To AP (infra.)	1	0	BSSID	SA	DA	not used
From AP (infra.)	0	1	DA	BSSID	SA	not used
WDS (bridge)	1	1	RA	TA	DA	SA

Tabla 6: Campos direcciones según sentido.

- Canal en el que está transmitiendo el AP.
- Contador de número de tramas de datos transmitidas y recibidas durante el intervalo. Con este campo se podrá saber cuánto tráfico ha generado el dispositivo.

- Contador de numero de tramas de datos de tamaño menor a 1000 bytes/trama, transmitidas y recibidas durante el intervalo. Este campo servirá para en la fase de análisis poder predecir el tipo de tráfico que ha estado cursando el dispositivo, texto, video, streaming, etc.
- Contador de numero de tramas de datos de tamaño entre 500 y 1000 bytes/trama transmitidas y recibidas durante el intervalo. Este campo servirá para en la fase de análisis poder predecir el tipo de tráfico que ha estado cursando el dispositivo, texto, video, streaming, etc.
- Contador de numero de tramas de datos de tamaño entre 300 y 500 bytes/trama transmitidas y recibidas durante el intervalo. Este campo servirá para en la fase de análisis poder predecir el tipo de tráfico que ha estado cursando el dispositivo, texto, video, streaming, etc.
- Contador de numero de tramas de datos de tamaño entre 10 y 300 bytes/trama transmitidas y recibidas durante el intervalo. Este campo servirá para en la fase de análisis poder predecir el tipo de tráfico que ha estado cursando el dispositivo, texto, video, streaming, etc.
- Nivel de potencia máxima y mínima detectadas en las tramas durante el intervalo. Observando la diferencia entre la máxima y mínima potencia recibidas, se puede considerar si el dispositivo se está moviendo o está fijo durante ese intervalo. Si la diferencia es mayor de 30 dbm se considera que se está moviendo.

Se puede incluir una monitorización activa en cada intervalo de tiempo para complementar el estado del dispositivo en cada intervalo. Como es sabido, para realizar dicha monitorización activa se necesita que el dispositivo, en este caso la Raspberry, este conectada a la red que se pretenda monitorizar, lo cual puede conllevar que sea necesaria algún tipo de autenticación para conectarse y solo se puede realizar monitorización activa en una red. Con esta monitorización activa y la pasiva se pueden sacar conclusiones comparando los resultados en la fase de análisis, pero solamente de una de las tres redes que se están monitorizando en modo pasivo.

Para resumir, podemos observar que esta tabla ha sido creada por el programa de forma automática facilitando su posterior análisis, por tanto, los comportamientos analizados de forma automatizada por el programa y almacenados en esta tabla son:

- Cantidad de tráfico generado por el dispositivo en cada intervalo de tiempo.
- Qué tipo de tráfico se puede considerar que está generando el dispositivo en cada intervalo de tiempo, en base al tamaño de la trama.
- El comportamiento del dispositivo en cada intervalo, de esta manera se podrá saber en qué periodo de tiempo la red está más activa, es decir, tiene más tráfico. También qué punto de acceso cursa más tráfico en cada franja horaria.
- Detectar si un dispositivo se está moviendo observando la máxima y la mínima potencia con la que se reciben las tramas, o si ha cambiado de punto de acceso al que estar conectado.

Se podría hacer un análisis por hora, día, semana o mes.

2.3.1.4. Estructura del programa

El programa customizado está estructurado de manera que pueda ser flexible en cuanto a reutilización, es decir, que se pueda usar para otros casos de forma simple cambiando poca cosa, además, está estructurado de la manera más óptima para su compresión.

Consta de un programa principal, llamado Main, que se encarga de ejecutar el programa, por otro lado, se han implementado cinco módulos, los cuales son utilizados por el programa principal para llevar a cabo la captura y procesamiento de las tramas.
En todos estos módulos se utilizan diversas librerías de Python para implementar las soluciones.

Las principales partes del programa se explicarán a continuación de forma detallada:

Módulo Main

Es el programa principal, contiene el código para capturar y analizar las tramas, desde aquí se llama al resto de módulos para realizar esta tarea. Aquí se explicará la función del programa completo, el resto de módulos complementan esta explicación entrando más en detalle en el cómo está realizado.

- **Entrada**

  Recibe la información por medio de un comando para ejecutarse, en este comando debe recibir los siguientes datos para hacerlo fácilmente adaptable a cualquier situación:

  a. Intervalo de monitorización: Tiempo (seg.) durante el cual se va a capturar y contabilizar tramas tanto de los Puntos de acceso como de los dispositivos.
  b. Numero de redes WIFI a monitorizar y sus correspondientes nombres (SSID)
  c. Reinicio del programa: Si es la primera vez que ejecuta el programa o es un reinicio, esta última opción el programa cogería los valores de entrada de la anterior ejecución y continuaría almacenando datos de las tramas en el punto donde se paró la ejecución anterior.

- **Funcionamiento**

  En la siguiente figura se muestra de forma general cómo funciona el programa.

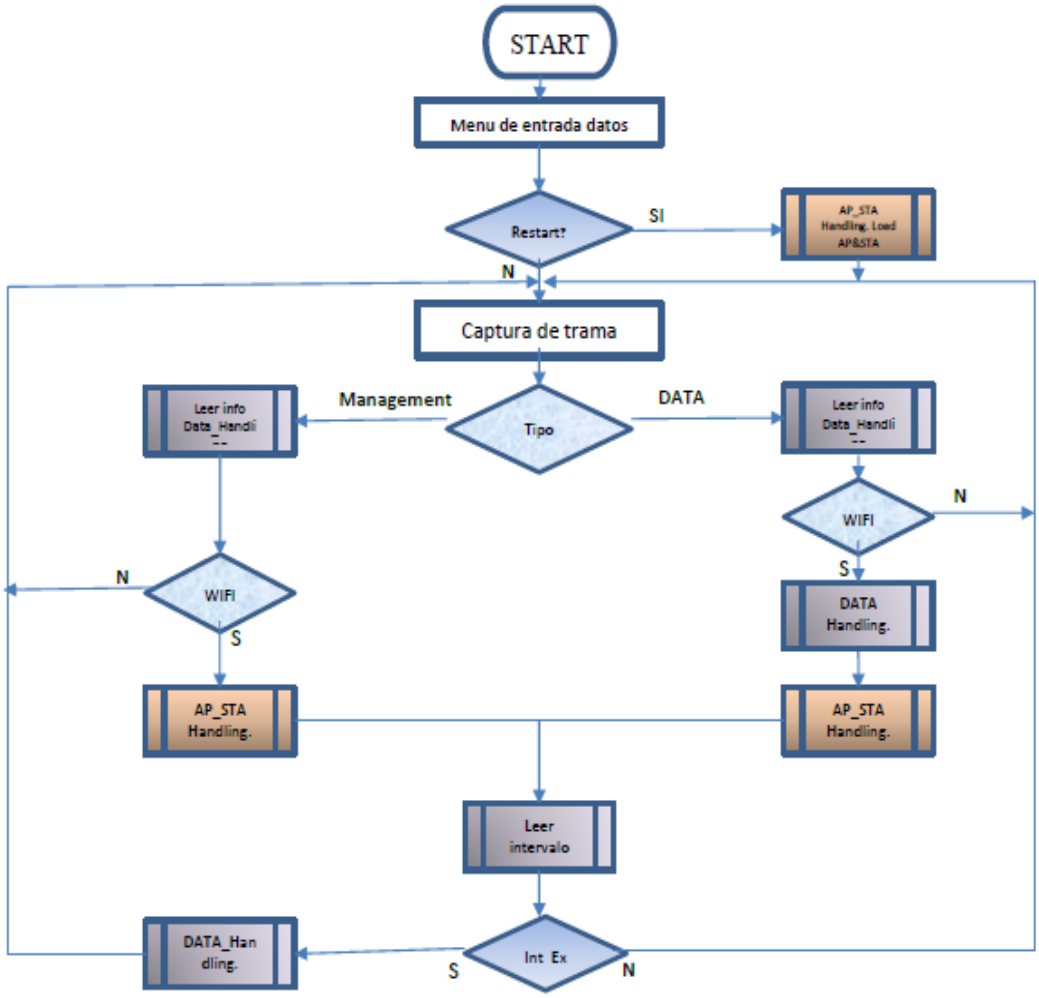


Figura 22: Diagrama de flujo del funcionamiento del programa principal.

Este programa comienza con un bucle While infinito, ejecutándose continuamente, se capturan las tramas de una en una y se comprueba que tipo de trama son, para según el tipo tratarlas de modo adecuado para sacar la información correspondiente.
Con las tramas de gestión(BEACON/PROBE_RESPONSE) se obtiene información de los puntos de acceso de las redes que se están monitorizando. La información obtenida es por ejemplo, BSSID, SSID, canal por el que está transmitiendo, señal con la que la trama es recibida, tipo de trama, subtipo de trama, etc.
Como se puede observar en el diagrama, la primera vez que se detecta una dirección física de un punto de acceso nueva(buscar_AP) se guarda en una tabla de la base de datos, con el objetivo de facilitar el posterior análisis teniendo en esa tabla los puntos de acceso detectados en la red de forma única.
Mediante las tramas de tipo datos, se analizarán los subtipos DATA, QoS DATA, NULL_DATA, QoS NULL_DATA, se obtiene información relevante sobre los dispositivos conectados a las redes monitorizadas. La principal información obtenida es BSSID, SSID, canal por el que se transmitió la trama, señal con la que es recibida la trama,tipo y subtipo de trama, las 4 direcciones MAC del estándar 802.11, etc. [13]

De la misma manera que se guardaban en una tabla los puntos de acceso únicos, cada vez que se detecte que un dispositivo con una dirección física nueva(buscar_STA) está cursando tramas en la red se guardará en otra tabla de la base de datos para tener en ella los dispositivos que en algún momento han estado conectados a las redes monitorizadas de forma única, de nuevo facilitando el posterior análisis.

Todas las tramas de datos procesadas son almacenadas en otra tabla de la base de datos para poder tener toda la información y poder obtener los mayores datos posibles para el posterior estudio. Además de capturar la información relevante de las tramas capturadas, el programa va contando las tramas procesadas.

Una vez tratada la trama capturada, se comprueba si el intervalo de comportamiento ha expirado, si ha expirado se llama a la función ‘*’loadtable’’,* ubicada en el módulo *‘’Intervalo_Handling’’*, donde se procederá a realizar un análisis de comportamiento durante el tiempo que se le haya asignado al intervalo. Como resultado habrá dos nuevas tablas en la base de datos, una con el análisis del comportamiento de los puntos de acceso y otra con el análisis de comportamiento de los dispositivos.

- Salida

Utilizando los módulos auxiliares implementados, se obtiene como resultado ejecutando este código main las diferentes tablas de la base datos, que será la base de datos utilizada para realizar el análisis de estas redes.

Una tabla con los puntos de acceso de las redes de forma única, otra tabla con los dispositivos conectados a las redes de forma única, dos tablas más, con el análisis del comportamiento de dichos dispositivos y puntos de acceso, respectivamente.
También habrá una tabla en la que se almacenarán todas las tramas capturadas.

Módulo AP_STA_CLASS

Para facilitar el tratamiento y manejo de los datos obtenidos se ha implementado este módulo, que contiene 2 clases dentro de él. Una clase para el tratamiento y manejo de los datos correspondientes a los puntos de acceso y otra para el tratamiento y manejo de los datos correspondientes a los dispositivos conectados a las redes monitorizadas.

- **ENTRADA**

Las entradas son las llamadas en el código main.

- **FUNCIONAMIENTO**

Este módulo consta de dos clases con sus correspondientes funciones.

- Clase Access_Point: Se define un objeto de este tipo por cada punto de acceso encontrado en nuestras redes. Se necesitan una serie atributos para inicializar un objeto de tipo Access_Point, estos atributos son los que se almacenarán en las tablas de la base de datos para su análisis.

```
class Access_point (object):
    'Clase para Access Points'
    numaps = 0
    def __init__(self, DIA_I, HORA_I, Frame_type, Frame_subtype, SSID, BSSID, Destination_add, Source_add, Receiver_add, Transmitter_add, STA_Status,
        DS_Status,Channel_AP,SSI_signal, N_BEACON, N_PROBE_RESPON, N_PROBE_REQUEST, N_Ass_Request, N_DATA, throughput1 ):
        self.DIA_I = DIA_I
        self.HORA_I = HORA_I
        self.Frame_type = Frame_type
        self.frame_subtype = Frame_subtype
```

Figura 23: Clase Punto de Acceso.

Dentro de esta clase se encuentran funciones para el manejo de las tramas cursadas de forma fácil e intuitiva:

1) Función contador de tramas. Esta función sirve para contar las tramas cursadas, comprueba el tipo de trama y aumenta el contador del tipo de trama correspondiente.
2) Función obtener contadores. Sirve para obtener los contadores de tramas.
3) Función reset contadores. Resetea los contadores de las tramas.

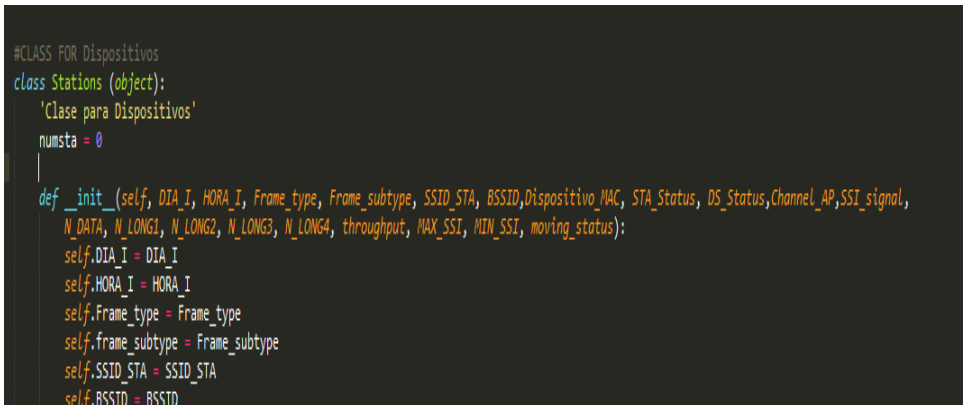
También hay funciones para el manejo del thorughput:

1) Función cargar_throughput.
2) Función get_throughput.
3) Funcion reset_thorughput.

Por último, funciones para manejar el estado:

1) Función getDisp_status. Para obtener del objeto los atributos SSID, BSSID, canal, señal.
2) Función setDisp_status. Para cambiar o dar valor a los atributos anteriores.
3) Funcion BSSID_exist.
4) Funcion BSSID_mostrar
5) Funcion SSID_mostrar

- Clase Stations: Se define un objeto de este tipo por cada dispositivo encontrado en nuestras redes. Se necesitan una serie atributos para inicializar un objeto de tipo Stations, estos atributos son los que se almacenarán en las tablas de la base de datos para su análisis.



```
#CLASS FOR Dispositivos
class Stations (object):
    'Clase para Dispositivos'
    numsta = 0

    def __init__(self, DIA_I, HORA_I, Frame_type, Frame_subtype, SSID_STA, BSSID,Dispositivo_MAC, STA_Status, DS_Status,Channel_AP,SSI_signal,
        N_DATA, N_LONG1, N_LONG2, N_LONG3, N_LONG4, throughput, MAX_SSI, MIN_SSI, moving_status):
        self.DIA_I = DIA_I
        self.HORA_I = HORA_I
        self.Frame_type = Frame_type
        self.frame_subtype = Frame_subtype
        self.SSID_STA = SSID_STA
        self.BSSID = BSSID
```

Figura 24: Clase Dispositivos.

Dentro de esta clase se encuentran funciones para el manejo de las tramas cursadas de forma fácil e intuitiva:

1) Función contador de tramas.
2) Función obtener contadores de tramas.
3) Función resetear contadores de tramas.

Para el manejo del estado del dispositivo:

1) Función getDispMAC.
2) Función getSTA_Status.
3) Función setDispStatus.
4) Función getDispStatus.
5) Función getBSSID.

Funciones para el manejo de la potencia de transmisión de la señal:

1) Función cargarSSI_signal.
2) Función getSSI_signal.
3) Función borrarSSI_signal.
4) Función maxSSI_signal. Calcula la SSI máxima.
5) Función minSSI_signal.

Además, para el manejo del estado de la movilidad.

1) Función setStatus_mov.
2) Función getStatus_mov.
3) Función resetStatus_mov.

Por último, funciones para el manejo del throughput:

1) Función cargarThroughput.
2) Función getThroughput.
3) Función resetThroughput.

Módulo AP_STA_Handling

Para el manejo de los objetos de tipo Access_Point y Station se ha implementado este módulo, consta de varias funciones.

- **ENTRADA**

El programa principal main, a la hora de tratar los objetos de tipo Access_Point o Station, hace uso de las funciones de este módulo.

- **FUNCIONAMIENTO**

Las funciones de las que consta este módulo son las siguientes:

1) Función buscarAP: Es utilizada desde el programa main, su función es verificar que el punto de acceso es la primera vez que se detecta o no, los atributos de entrada de esta función es precisamente la información obtenida de la trama capturada. Si es la primera vez que se ha detectado este punto de acceso(BSSID) se crea un objeto de tipo Access_Point que contendrá en sus atributos toda la información recabada con la trama y se almacena en la tabla donde estarán los puntos de acceso detectados en la red de forma única. Si el punto el acceso ya se había detectado se actualiza la información de ese objeto punto de acceso, es decir, los contadores de tramas, throughput, etc.

2) Función buscarSTA(dispositivo): Es utilizada desde el programa main, su función es verificar que el dispositivo es la primera vez que se detecta o no, los atributos de entrada de esta función es precisamente la información obtenida de la trama capturada. Si es la primera vez que se ha detectado este dispositivo(STA_Dispositivo_MAC) se crea un objeto de tipo Station que contendrá en sus atributos toda la información recabada con la trama y se almacena en la tabla donde estarán los dispositivos conectados a la red de forma única. Si el dispositivo existe incrementamos el contados de tramas de datos para ese dispositivo, y los contadores de tramas según tamaño, llamando a la función correspondiente del objeto

3) Función loadAP: Esta función es utilizada en el programa principal cuando este se ha reiniciado. Su función es recuperar la información que hay en las tablas de la base de datos referente a puntos de acceso y cargar esta información en los obejetos de puntos de acceso. Sirve para poder continuar con la monitorización en caso de parada.

4) Función loadSTA: Esta función es utilizada en el programa principal cuando este se ha reiniciado. Su función es recuperar la información que hay en las tablas de la base de datos referente a los dispositivos y cargar esta información en los objetos de dispositivo. Sirve para poder continuar con la monitorización en caso de parada.

- **DIAGRAMA DE FLUJO**

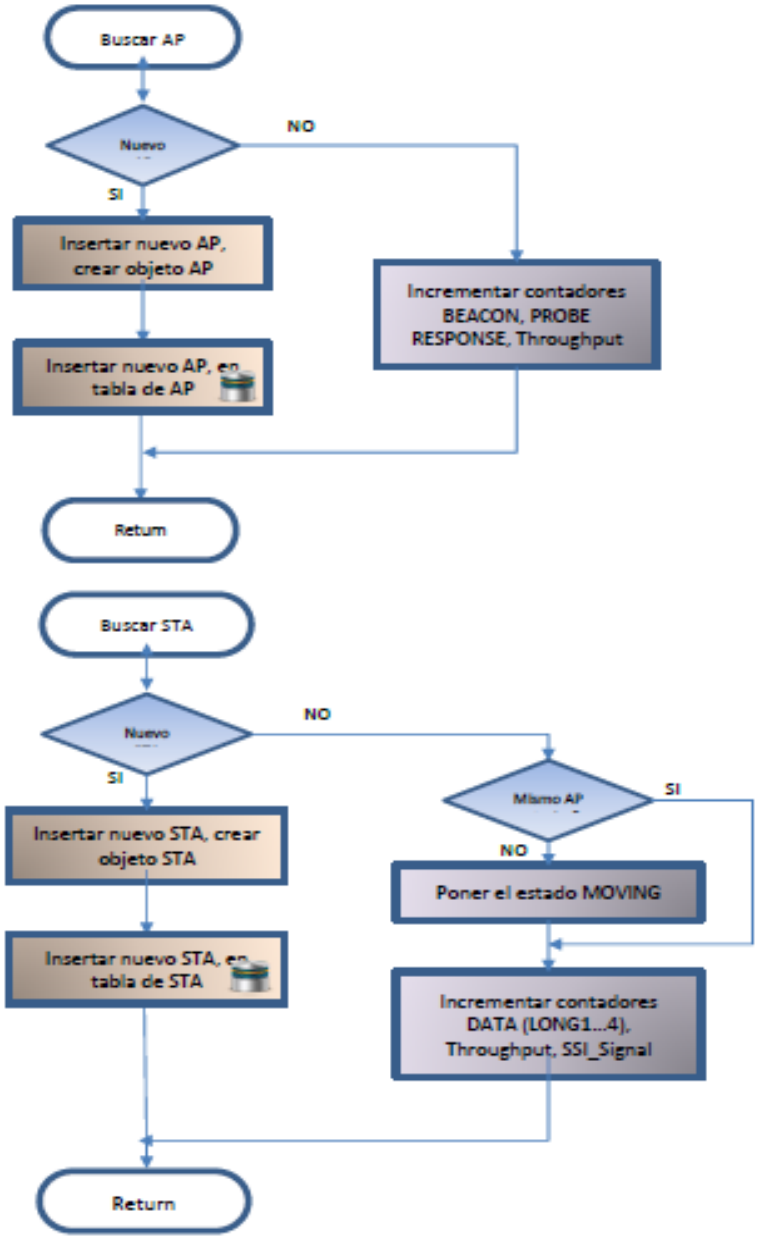


Figura 25: Diagrama de flujo de módulo AP_STA_HANDLING.

- **SALIDA**

Este módulo es usado en el programa principal main para crear las tablas que contienen los puntos de acceso únicos de las redes monitorizadas y los dispositivos únicos que en algún momento han estado conectados a las redes monitorizadas.

Además, se encarga de crear objetos de tipo Access_Point o Station según corresponda y mantiene actualizada la información de los contadores de tramas, throughput y la señal con la que se reciben las tramas.

Tabla: frames_802_AP2 Nuevo registro Borrar registro

	STA_Status	DIA_I	HORA_I	SSID1	Fabricante	Channel_AP	SSI_signal	BSSID
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	Access Point	26/07/17	09:52:34	SSID-3	Hewlett Packard	1	-61	BSSID-1
2	Access Point	26/07/17	09:52:34	SSID-1	Hewlett Packard	1	-60	BSSID-2
3	Access Point	26/07/17	09:52:34	SSID-2	Hewlett Packard	1	-62	BSSID-3
4	Access Point	26/07/17	09:53:29	SSID-2	Hewlett Packard	6	-62	BSSID-4
5	Access Point	26/07/17	09:53:29	SSID-3	Hewlett Packard	6	-62	BSSID-5
6	Access Point	26/07/17	09:53:29	SSID-1	Hewlett Packard	6	-61	BSSID-6
7	Access Point	26/07/17	09:53:29	SSID-2	Hewlett Packard	11	-62	BSSID-7
8	Access Point	26/07/17	09:53:29	SSID-3	Hewlett Packard	11	-62	BSSID-8
9	Access Point	26/07/17	09:53:29	SSID-1	Hewlett Packard	11	-61	BSSID-9
10	Access Point	08/08/17	08:46:29	SSID-2	Hewlett Packard	1	-66	BSSID-10
11	Access Point	10/08/17	15:55:32	SSID-2	Hewlett Packard	1	-69	BSSID-11
12	Access Point	17/08/17	09:04:43	SSID-3	Hewlett Packard	1	-66	BSSID-12

Figura 26: Tabla que contiene los puntos de acceso.

	DIA_I	HORA_I	SSID	Dispositivo_MAC	BSSID	Fabricante	DS_Status	Channel_
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	17/08/17	10:06:40	SSID-2	STA344	BSSID-4	zte corporation	FROM_STA_T...	6
2	26/07/17	11:46:34	SSID-2	STA44	BSSID-3	Xiaomi Communic...	FROM_DS_TO...	1
3	27/07/17	08:24:50	SSID-2	STA93	BSSID-7	Xiaomi Communic...	FROM_STA_T...	11
4	17/08/17	12:46:44	SSID-2	STA350	BSSID-3	Xiaomi Communic...	FROM_DS_TO...	1
5	27/07/17	08:14:28	SSID-2	STA92	BSSID-3	WISOL	FROM_DS_TO...	1
6	02/08/17	11:59:58	SSID-2	STA244	BSSID-3	WISOL	FROM_DS_TO...	1
7	16/08/17	17:34:26	SSID-3	STA339	BSSID-8	TCT mobile ltd	FROM_STA_T...	11
8	26/07/17	09:52:41	SSID-2	STA4	BSSID-3	Sony Mobile Com...	FROM_STA_T...	1
9	26/07/17	11:01:40	SSID-2	STA30	BSSID-3	Sony Mobile Com...	FROM_DS_TO...	1
10	26/07/17	11:21:53	SSID-2	STA35	BSSID-7	Sony Mobile Com...	FROM_STA_T...	1
11	26/07/17	13:00:22	SSID-2	STA57	BSSID-4	Sony Mobile Com...	FROM_DS_TO...	6
12	26/07/17	16:44:42	SSID-2	STA81	BSSID-3	Sony Mobile Com...	FROM_STA_T...	1
13	27/07/17	10:54:21	SSID-3	STA111	BSSID-1	Sony Mobile Com...	FROM_STA_T...	1

Figura 27: Tabla Dispositivos.

Módulo DB_HANDLING

Este módulo es utilizado por el programa principal para hacer una copia de la base de datos, de esta manera se pretende asegurar los datos en caso de que ocurra algún problema, como que la base de datos se corrompa, se produzca un apagón y la Raspberry se quede sin alimentación, etc. Así se evitará perder todos los datos monitorizados hasta ese momento.

Módulo INTERVALO_HANDLING

Este módulo es utilizado por el programa principal para controlar el intervalo de comportamiento, además es utilizado para analizar el comportamiento de los puntos de acceso y dispositivos detectados así como cargar esta información en las correspondientes tablas de la base de datos.

Las funciones que contiene este módulo son:

1) Función tiempo expirado: Sirve para comprobar si ha expirado el intervalo de comportamiento, previamente establecido.
2) Función de carga de las tablas de comportamiento: Está función es usada por el programa principal justo después de saber que ha expirado el tiempo del intervalo. Sirve para cargar toda la información que se ha obtenido de las tramas capturadas, tanto referente a los puntos de acceso como de los dispositivos y lo almacena en la tabla de la base de datos que corresponda.
   Se producirá un registro por cada hora, ya que el intervalo utilizado en esta monitorización ha sido de una hora.
   En la tabla de comportamiento de puntos de acceso se almacena información como numero de tramas cursadas, throughput,etc, durante esa hora.
   En la tabla de comportamiento de los dispositivos se almacena información como tramas de datos cursadas, divididas por tamaño, potencia de la señal máxima y mínima etc.

STA_Status	DIA_I	HORA_I	SSID	Intervalo	BSSID	Channel_AP	SSI_signal	N_BEACON	_PROBE_RESPO
Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
Access Point	29/05/17	11:06:09	SSID-2	11:00	BSSID-1	1	-54	6828	3888
Access Point	29/05/17	11:06:09	SSID-3	11:00	BSSID-2	1	-54	6520	3334
Access Point	29/05/17	11:06:09	SSID-1	11:00	BSSID-3	1	-54	6481	3727
Access Point	29/05/17	11:06:09	SSID-1	11:00	BSSID-9	6	-69	18	78
Access Point	29/05/17	11:06:09	SSID-2	11:00	BSSID-4	11	-49	22	78
Access Point	29/05/17	11:06:09	SSID-3	11:00	BSSID-5	11	-45	25	75
Access Point	29/05/17	11:06:09	SSID-1	11:00	BSSID-6	11	-52	22	76
Access Point	29/05/17	11:06:09	SSID-3	11:00	BSSID-7	6	-66	22	67
Access Point	29/05/17	11:06:10	SSID-2	11:00	BSSID-8	6	-66	13	67
Access Point	29/05/17	12:06:09	SSID-2	12:00	BSSID-1	1	-57	7328	3880
Access Point	29/05/17	12:06:09	SSID-3	12:00	BSSID-2	1	-60	7081	3455
Access Point	29/05/17	12:06:09	SSID-1	12:00	BSSID-3	1	-61	7412	3722
Access Point	29/05/17	12:06:09	SSID-1	12:00	BSSID-9	6	-61	24	70
Access Point	29/05/17	12:06:09	SSID-2	12:00	BSSID-4	11	-48	29	65
Access Point	29/05/17	12:06:09	SSID-3	12:00	BSSID-5	11	-52	25	65
Access Point	29/05/17	12:06:09	SSID-1	12:00	BSSID-6	11	-51	21	58
Access Point	29/05/17	12:06:09	SSID-3	12:00	BSSID-7	6	-57	19	68

Figura 28: Tabla de comportamiento de los dispositivos.

HORA_U	Intervalo	SSID	Dispositivo_MAC	STA_Status	TA_moving_stat	DS_Status	Channel_AP	N_DATA	N_LONG1	N_LONG2	N_LONG3	N_
Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
10:52:34	10	b'EWA@INTE...	STA1	Active	Fijo	FROM_STA_T...	1	11632	0	0	0	1163
10:52:34	10	b'EWA@INTE...	STA2	Connected	Fijo	FROM_STA_T...	1	1124	13	7	8	1096
10:52:34	10	b'EWA@INTE...	STA3	Active	Fijo	FROM_STA_T...	1	636	0	0	0	636
10:52:34	10	b'EWA@INTE...	STA4	Connected	Fijo	FROM_STA_T...	1	1792	13	3	7	1769
10:52:34	10	b'EWA@INTE...	STA5	Active	Fijo	FROM_STA_T...	1	173	0	0	0	173
10:52:34	10	b'EWA@INTE...	STA6	Pasive	Fijo	FROM_DS_TO...	1	67	2	1	6	58
10:52:34	10	b'EWA@ECN'	STA7	Connected	Fijo	FROM_DS_TO...	11	11	2	0	0	9
10:52:35	10	b'EWA@INTE...	STA8	Active	Fijo	FROM_STA_T...	12	17	0	0	0	17
10:52:35	10	b'EWA@INTE...	STA9	Connected	Fijo	FROM_DS_TO...	1	128	4	0	2	122
10:52:35	10	b'EWA@ECN'	STA10	Connected	Moving	FROM_STA_T...	1	49	0	0	0	49
10:52:35	10	b'EWA@INTE...	STA11	Connected	Fijo	FROM_STA_T...	1	2018	15	0	6	1997
10:52:35	10	b'EWA@INTE...	STA12	Active	Fijo	FROM_STA_T...	1	36	0	0	0	36
10:52:35	10	b'EWA@INTE...	STA13	Pasive	Fijo	FROM_DS_TO...	1	22	2	0	0	20
10:52:35	10	b'EWA@INTE...	STA14	Connected	Fijo	FROM_STA_T...	1	58	2	0	0	56
10:52:35	10	b'EWA@ECN'	STA15	Connected	Moving	FROM_STA_T...	1	202	29	6	4	163
10:52:35	10	b'EWA@INTE...	STA16	Pasive	Fijo	FROM_DS_TO...	1	39	0	0	0	39
10:52:35	10	b'EWA@INTE...	STA17	Connected	Moving	FROM_STA_T...	1	1512	230	66	39	1177

Figura 29: Tabla de comportamiento de los puntos de acceso.

- **DIAGRAMA DE FLUJO**

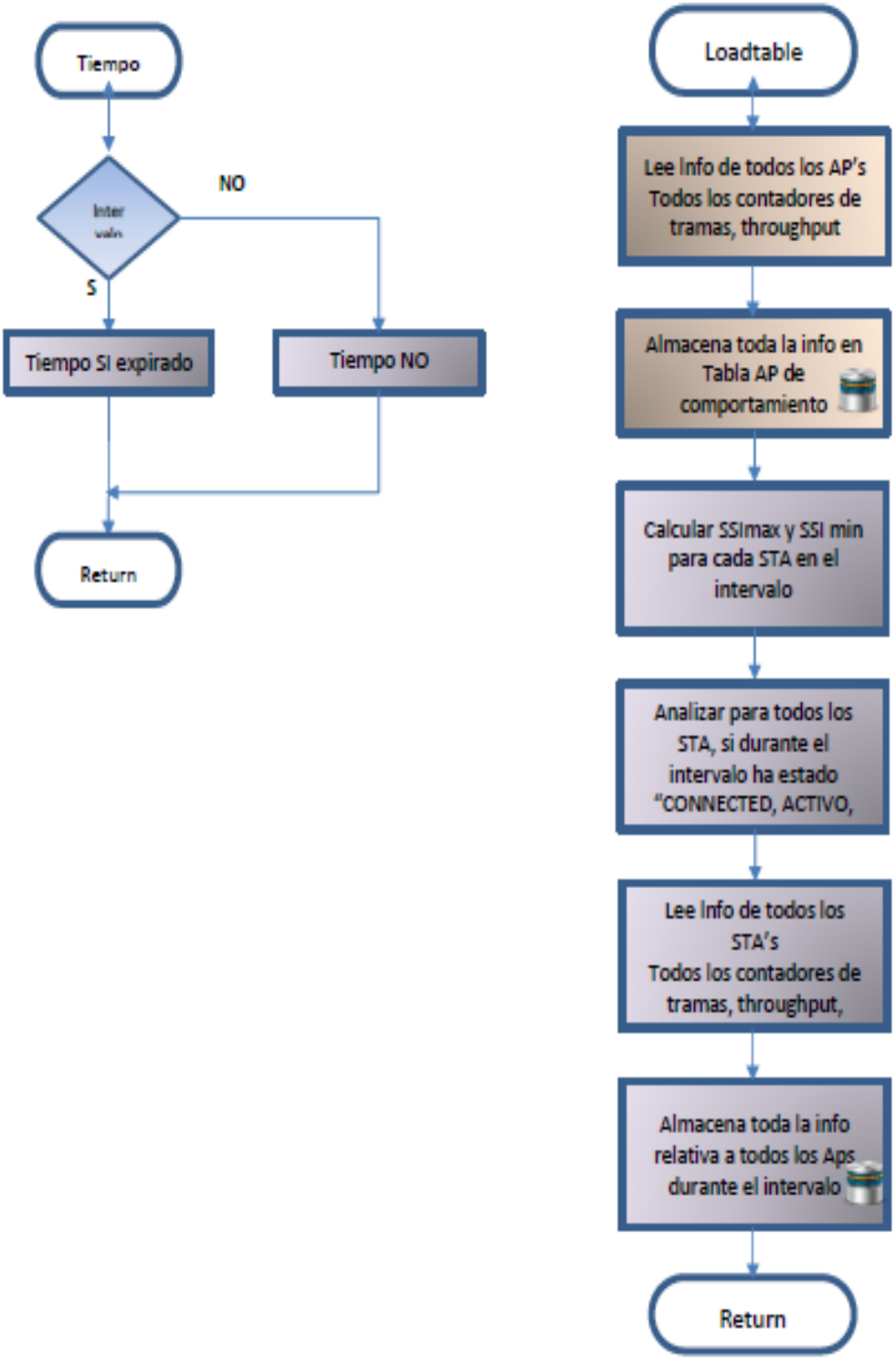


Figura 30: Diagrama de flujo del módulo Intervalo_Handling.

Módulo DATA_HANDLING

Este módulo tiene como misión principal el filtrado de las tramas multicast, para evitar que el programa capture y analice tramas que contengan direcciones multicast y que en el estudio no aportan nada relevante, ya que no sabemos a que dispositivos en concreto van dirigidas. Su misión es filtrarlas para que no sean tratadas. Las direcciones consideradas multicast son las siguientes:

Ethernet multicast address	Type Field	Usage
01-00-0C-CC-CC-CC		CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)
01-00-0C-CC-CC-CD		Cisco Shared Spanning Tree Protocol Address
01-80-C2-00-00-00		Spanning Tree Protocol (for bridges) IEEE 802.1D
01-80-C2-00-00-00, or01-80-C2-00-00-03, or 01-80-C2-00-00-0E	0x88CC	Link Layer Discovery Protocol
01-80-C2-00-00-08	0x0802	Spanning Tree Protocol (for provider bridges) IEEE 802.1ad
01-80-C2-00-00-01	0x8808	Ethernet flow control (Pause frame) IEEE 802.3x
01-80-C2-00-00-02	0x8809	Ethernet OAM Protocol IEEE 802.3ah (A.K.A. "slow protocols")
01-80-C2-00-00-30 - 01-80-C2-00-00-3F	0x8902	Ethernet CFM Protocol IEEE 802.1ag
01-00-5E-00-00-00 - 01-00-5E-7F-FF-FF	0x0800	IPv4 Multicast (RFC 1112), insert the low 23 Bits of the multicast IPv4 Address into the Ethernet Address (RFC 7042 2.1.1.)
33-33-xx-xx-xx-xx	0x86DD	IPv6 Multicast (RFC 2464), insert the low 32 Bits of the multicast IPv6 Address into the Ethernet Address (RFC 7042 2.3.1.)
01-0C-CD-01-00-00 01-0C-CD-01-01-FF	0x88B8	IEC 61850-8-1 GOOSE Type 1/1A
01-0C-CD-02-00-00 01-0C-CD-02-01-FF	0x88B9	GSSE (IEC 61850 8-1)
01-0C-CD-04-00-00 01-0C-CD-04-01-FF	0x88BA	Multicast sampled values (IEC 61850 8-1)
01-1B-19-00-00-00, or 01-80-C2-00-00-0E	0x88F7	Precision Time Protocol (PTP) version 2 over Ethernet (Layer-2)

Tabla 7: Direcciones multicast.

- **DIAGRAMA DE FLUJO**

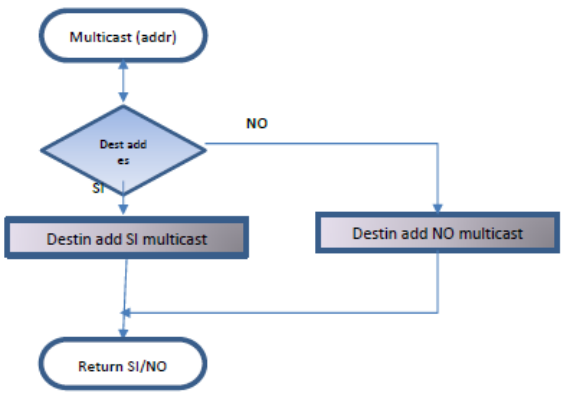


Figura 31: Diagrama de flujo del módulo Data_Handling.

LIBRERÍAS

Para la implementación de la solución completa se han utilizado diferentes librerías de Python, estas librerías han sido utilizadas por todos los módulos que forman el programa. Las librerías usadas son las siguientes:

- Socket
- Math
- Binascii
- Sqlite3
- Datetime
- Time
- Shlex
- Subprocess
- Multiprocessing import Process

2.3.2. Fase de validación

2.3.2.1. Objetivo

Para probar la fiabilidad del sniffer, se han realizado unas comprobaciones con herramientas comerciales y medidas de tiempo. Las pruebas a realizar están dirigidas para comprobar si las medidas hechas por nuestro sniffer son comparables a la realizadas por estas herramientas.

2.3.2.2. Medidas

- **Medidas de números de tramas beacon y de datos cursadas por los APs**

Consiste en comparar los contadores de nuestro sniffer con los contadores de airodump-ng. Lo hacemos durante un intervalo de tiempo.

Fig. Resultado con airodump-ng

Punto de Acceso

BSSID	First time seen	Last time seen	channel	Speed	Privacy	Cipher	Authentication	Power	# beacon	# IV
6C:19:8F:BF:87:69	2017-05-23 09:48:57	2017-05-23 11:31:42	11	54	WPA2WPA	CCMP TKIP	PSK	-40	42653	66474

Station MAC	First time seen	Last time seen	Power	# packets	BSSID	Probed ESSIDs
E8:2A:EA:98:84:56	2017-05-23 10:04:22	2017-05-23 11:23:11	-36	41191	6C:19:8F:BF:87:69	
B8:27:EB:22:0B:41	2017-05-23 09:49:27	2017-05-23 11:30:10	-39	487	6C:19:8F:BF:87:69	
28:C2:DD:9A:31:DD	2017-05-23 09:48:58	2017-05-23 11:31:04	-68	18211	6C:19:8F:BF:87:69	dlink-8767
E0:5F:45:11:DF:7B	2017-05-23 09:49:58	2017-05-23 11:31:40	-68	2948	6C:19:8F:BF:87:69	
4C:74:03:6E:D9:95	2017-05-23 09:48:58	2017-05-23 11:31:40	-44	623	6C:19:8F:BF:87:69	
C8:F6:50:97:56:50	2017-05-23 09:49:27	2017-05-23 11:31:20	-42	1612	6C:19:8F:BF:87:69	
EC:08:6B:1F:02:49	2017-05-23 09:48:58	2017-05-23 11:31:35	0	236	6C:19:8F:BF:87:69	

Figura 32: Resultado con Airodump-ng.

DIA_I	HORA_I	SSID	BSSID	Channel_AP	SSI_signal	N_BEACON	N_PROBE_RESPON	N_DATA
23/05/17	10:03:43	b'dlink-8767'	6c:19:8f:bf:87:69	11	-35	7807	2012	4305
23/05/17	10:18:43	b'dlink-8767'	6c:19:8f:bf:87:69	11	-36	7446	1966	13932
23/05/17	10:33:43	b'dlink-8767'	6c:19:8f:bf:87:69	11	-36	7247	1979	11860
23/05/17	10:48:43	b'dlink-8767'	6c:19:8f:bf:87:69	11	-38	6868	1864	15719
23/05/17	11:03:43	b'dlink-8767'	6c:19:8f:bf:87:69	11	-29	6149	1409	9636
23/05/17	11:18:43	b'dlink-8767'	6c:19:8f:bf:87:69	11	-37	7042	1823	9799

Figura 33: Resultado con sniffer. DB SQlite3 AP1.

RESULTADOS:

- El periodo para la validación ha sido de 90 min.
- Nº tramas beacons detectadas Airodump-ng: 42.653.
- Nº tramas beacons detectadas por el sniffer: 42.559
- Desviacion aproximada 0,3%/90min
- Nº tramas data detectadas Airodump-ng: 65.308.
- Nº tramas data detectadas por el sniffer: 65.251
- Desviacion aproximada: 0,1% / 90min

CAPÍTULO III

3. ANÁLISIS

En este capítulo se va a realizar un análisis de los resultados obtenidos mediante gráficas realizadas en base a consultas a la base de datos.

Se han realizado dos monitorizaciones en una planta de oficinas, mencionada en detalle en el punto *2.1.2*.

3.1. Escenario 1

Las principales características de este escenario son las siguientes:

Periodo	29 Mayo – 3 Julio
Ventana temporal	1 hora
Número de dispositivos totales	336
Número de puntos de acceso totales	9
Número de redes	3

Tabla 8: Características escenario 1.

Se monitorizan 3 redes simultáneamente:

- Red 1: Red Laptops, 189 usuarios detectados.
- Red 2: Red Internet, 130 usuarios detectados.
- Red 3: Red Guests, 7 usuarios detectados.

El análisis se centrará en las redes laptops e internet, debido a que los datos obtenidos en la red guests no son suficientes para sacar ningún tipo de conclusión.

3.1.1. Análisis de comportamiento según la presencia de los dispositivos

Se pretende estudiar el comportamiento respecto a la presencia de los dispositivos conectados a las redes monitorizadas.

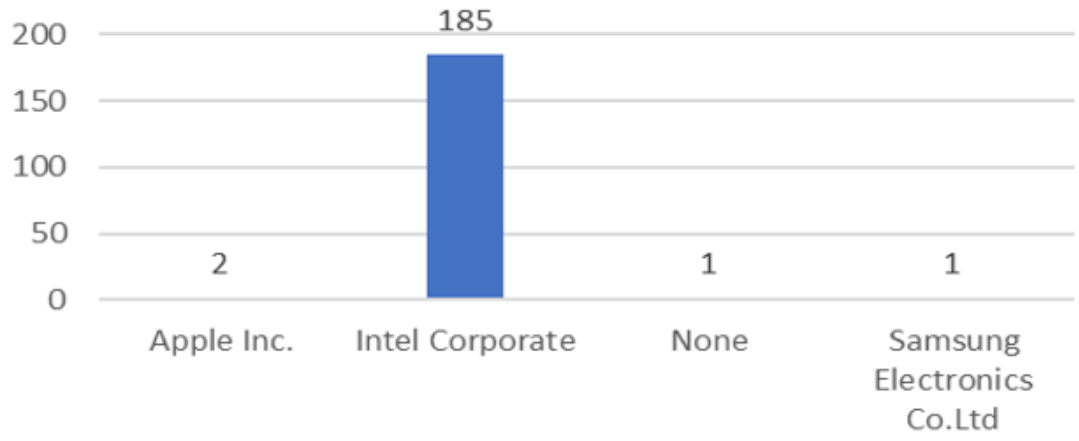


Figura 34: Gráfica que representa el número de usuarios conectados a la Red Laptops según la marca del dispositivo utilizado para la conexión.

Se puede observar que de 189 dispositivos totales conectados a esta red 185 eran tarjetas Wireless LAN Intel Corporate, 2 Apple Inc, 1 Samsung y otro desconocido. Esto certifica que efectivamente en esta red están conectados los laptops corporativos, con su Wireless LAN adapter (Wireless Network Connection) Intel Dual band Wireless-N.

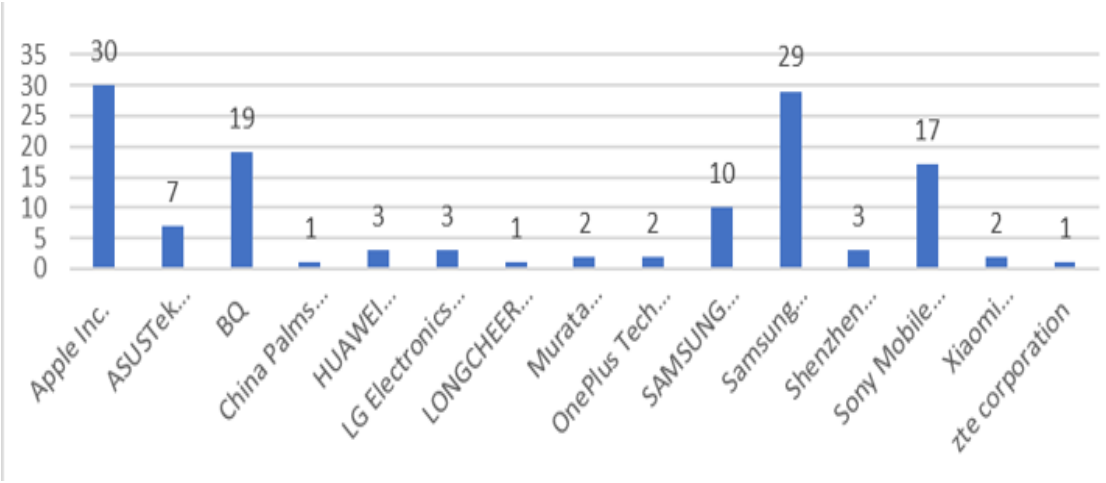


Figura 35: Gráfica que representa el número de usuarios conectados a la Red Internet según la marca del dispositivo utilizado para la conexión.

En figura 35 se pueden observar que los dispositivos conectados son de diferentes marcas, de teléfonos móviles, tablets, etc. Esta información tiene un valor comercial orientativo para ver que marca de dispositivos tienen mayor implantación en el mercado, en nuestro caso observamos que los más numerosos son de Apple, BQ, Samsung y Sony.

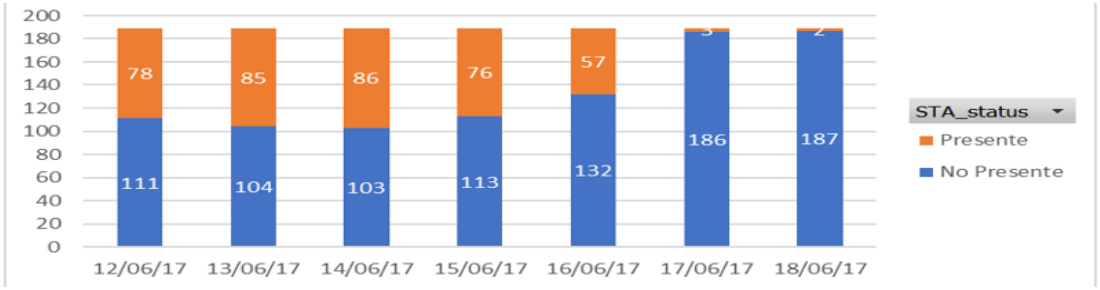


Figura 36: Gráfica que representa la presencia de los dispositivos en la Red Laptops durante una semana de lunes a domingo.

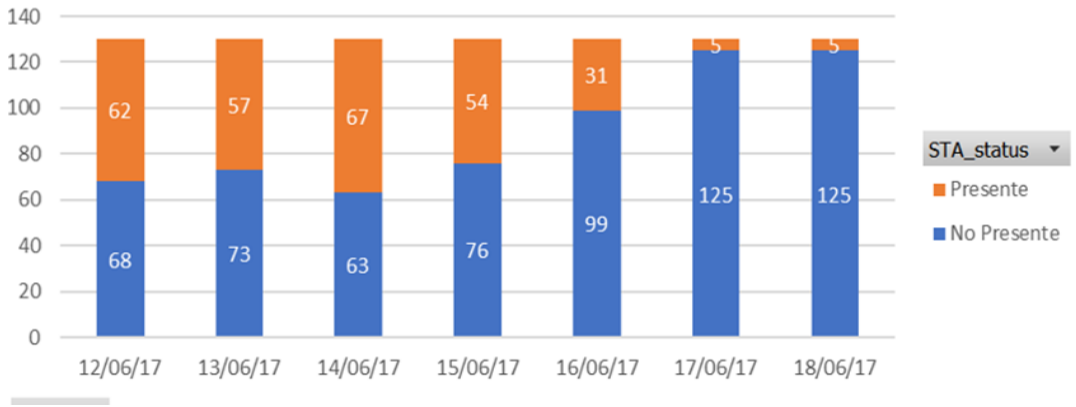


Figura 37: Gráfica que representa la presencia de los dispositivos en la Red Internet durante una semana, de lunes a domingo.

Se consideran presentes, los dispositivos que están cursando tráfico en la red. En ambas gráficas se puede observar que la presencia de los dispositivos disminuye el sábado y el domingo. Además, el viernes se aprecia un descenso de la presencia en comparación con el resto de la semana, debido a que es un día en el que muchos usuarios deciden trabajar desde sus casas. Este tipo de información permitiría valorar el uso del espacio de oficina, basados en que días hay más presencia de empleados, y así tomar decisiones futuras en cuanto a costes de infraestructura invertido por la empresa.

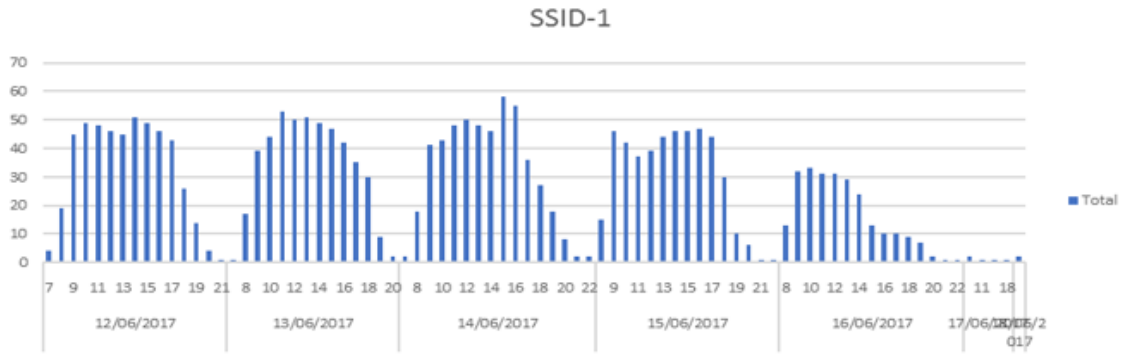


Figura 38: Gráfica que representa la presencia de los dispositivos en la Red Laptops durante una semana y los días divididos en intervalos de 2 horas.

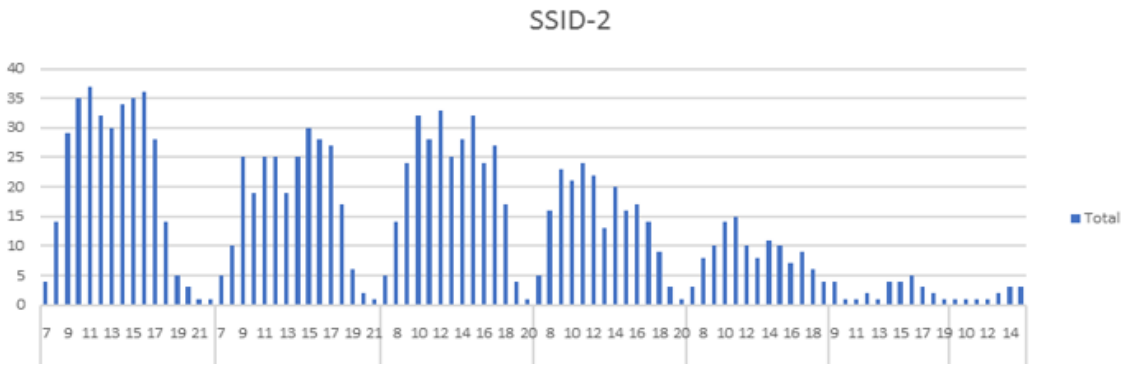


Figura 39: Gráfica que representa la presencia de los dispositivos en la Red Internet durante una semana y los días divididos en intervalos de 2 horas.

El análisis esta realizado sobre los dispositivos conectados y activos, es decir, los dispositivos que están cursando tráfico. En ambas gráficas (Fig 38 y 39), de nuevo se puede comprobar que el fin de semana no hay tráfico cursándose, debido a ello ni siquiera aparecen esos días completos en la gráfica. Además, podemos ver que de lunes a jueves la franja horaria donde se detecta el tráfico es aproximadamente de 8:00 a 19:00, cuando desciende considerablemente. Mientras que el viernes es de 8:00 a 16:00. Esta información resulta interesante para ver el comportamiento de los usuarios durante la franja horaria de la jornada laboral. En este caso es bastante homogénea, ya que la jornada laboral así lo es, en otros ámbitos como por ejemplos comercios, lugares públicos, etc, esta información podría ayudar a saber cuándo los clientes son más numerosos y poder reforzar los comercios con más empleados.

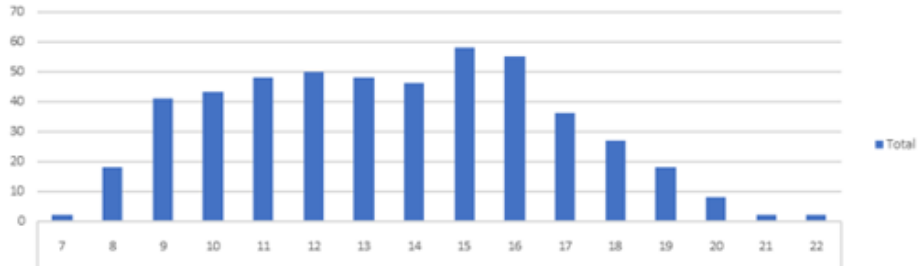


Figura 40: Gráfica de comportamiento de los dispositivos durante un día en la Red Laptops.

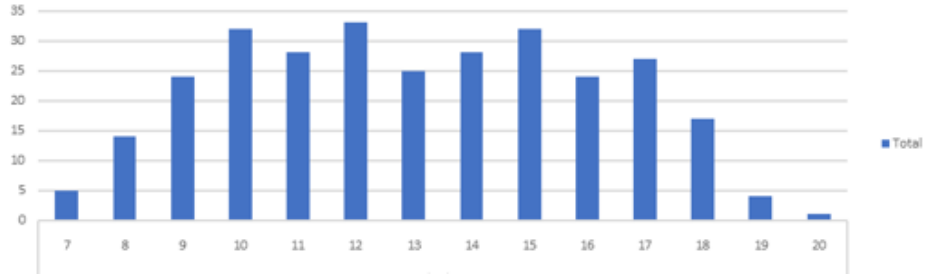


Figura 41: Gráfica de comportamiento de los dispositivos durante un día en la Red Internet.

Con estas gráficas (Fig 40 y 41) pretende analizar el comportamiento de los usuarios durante un día laborable cualquiera. En este caso se puede observar que se empieza a cursar tráfico en ambas redes a las 8:00 y a partir de las 18:00 empieza a descender, podemos concluir que la jornada laboral en esta oficina es aproximadamente de 8:00 a 18:00. Además, que las horas donde hubo mayor tráfico fueron de 10:00 a 13:00, donde se ve un pequeño descenso.

3.1.2. Análisis de tráfico cursado por las redes

Se va a analizar la cantidad de tráfico cursado por las redes monitorizadas. Para poder sacar conclusiones del tipo de tráfico cursado por las redes se van a tener en cuenta los campos de longitud de las tramas:

- Tramas de longitud LONG4: Son las tramas de tamaño de 100 a 300 bytes.
- Tramas de longitud LONG3: Son las tramas de tamaño de 300 a 500 bytes.
- Tramas de longitud LONG2: Son las tramas de tamaño de 500 a 1000 bytes.
- Tramas de longitud LONG1: Son las tramas de tamaño de más de 1000 bytes.

Para poder sacar conclusiones del tipo de tráfico cursado por las redes se van a tener en cuenta la longitud de las tramas en bytes. Se ha estimado que dependiendo el tamaño de la trama esta pertenecerá a un tipo de tráfico diferente según la tabla 9.

	Tipo de Trafico	Tipo de trama en funcion de su longitud			
1.- Usuario de laptops		LONG1	LONG2	LONG3	LONG4
Correo electronico	Texto			X	X
	Envio de documentos, presentaciones	X	X		
Skype	Texto			X	X
	Conf & multiconf AUDIO&VIDEO	X			
Navegacion Intranet/Internet	Descargas de documentación y subida de documentos en servidores o disco	X			
2.- Usuario de terminales moviles					
Correo electronico	texto			X	X
Whatsapp	texto			X	X
	Imágenes Y/O video	X			

Tabla 9: Tipo de tráfico según su longitud.

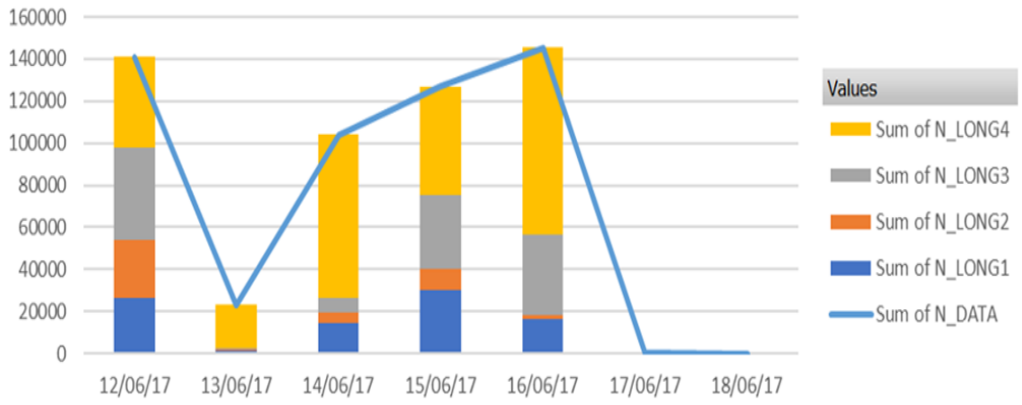


Figura 42: Número de tramas de DATA y su tamaño cursadas en la red Laptop en una semana.

En esta gráfica (Fig 42) se observa diversidad en el tipo de tráfico, ya que si nos fijamos en los tipos de tramas enviadas por día dependiendo de su tamaño se ve que es homogéneo.

Se comprueba también que el tráfico durante el fin de semana es nulo.

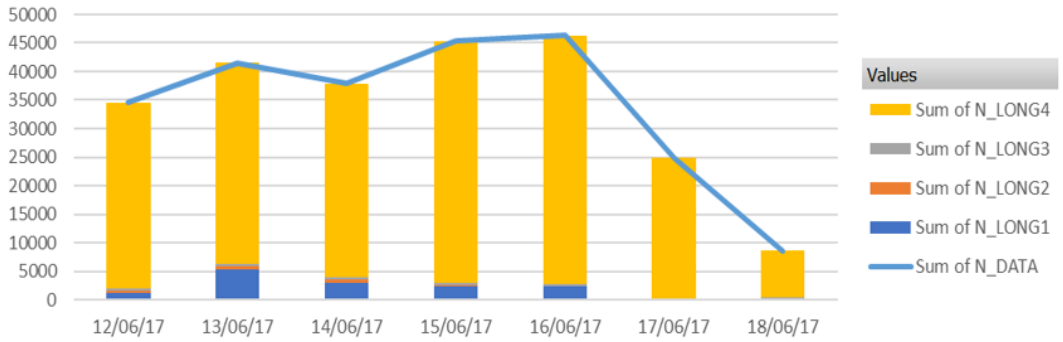


Figura 43: Número de tramas de DATA y su tamaño cursadas en la red Internet en una semana.

En el caso de la red de internet, donde se conectan los dispositivos que no son laptops corporativos, se puede comprobar que la mayoría de tráfico cursado es de tramas de tamaño N_LONG4, es decir, de menos de 300 bytes, lo cual significa que son tramas de datos del estilo de mensajes de texto.

Se puede observar algo de tráfico el fin de semana, puede ser debido a tráfico cursado por impresoras y dispositivos de la oficina de forma automática, sin necesidad de interacción con usuarios.

Nótese que la diferencia de tramas cursadas en ambas redes, en la red Laptop se multiplica por diez el número de tramas cursadas con respecto a la red Internet, esto es debido a que los laptops corporativos producen más tráfico, ya que son la herramienta de trabajo principal en la oficina. La red Internet está más relacionada con smartphones, tablets, impresoras… Por tanto, las tramas cursadas en esta red con tipo mensajes de whatsapp, correo electrónico, etc.

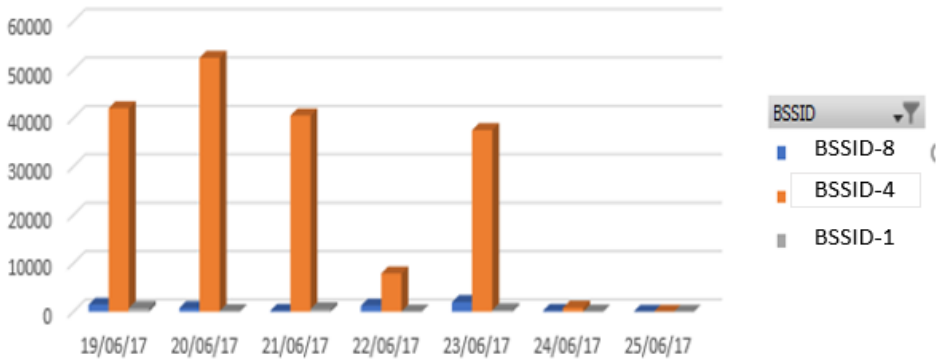


Figura 44: Gráfica con la cantidad de tramas cursadas por los puntos de acceso en la Red Internet durante una semana de lunes a domingo.

Observamos qué en esta red (Fig 44), la mayoría del tráfico es cursado por en punto de acceso con dirección física BSSID-4. Podemos deducir que esto es debido a que de los 3 puntos de acceso que tiene la red Internet, el punto de acceso cuya dirección física es BSSID-4 es el que está situado más cerca de la Raspberry, es del que recibe más cantidad de tramas y con mayor calidad. Si se hubiese hecho el estudio con 3 Raspberries cada una de ellas situada próxima a un punto de acceso se habría observado que los tres puntos de acceso de las redes tendrían aproximadamente el mismo tráfico.

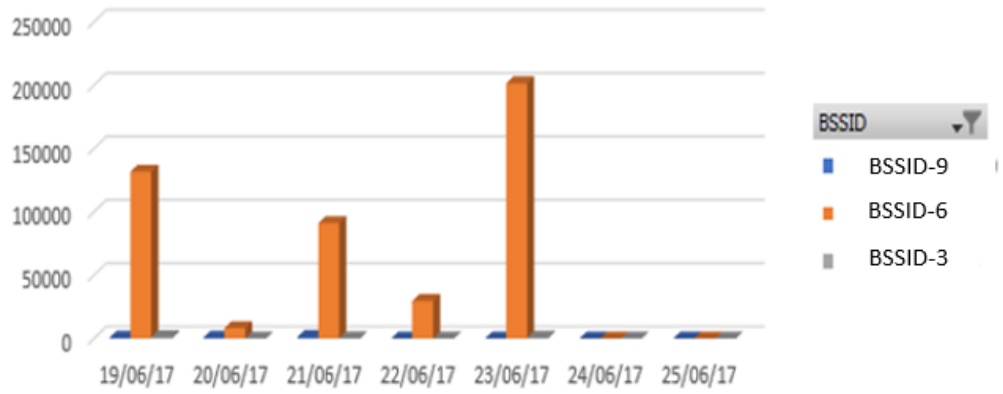


Figura 45: Gráfica con la cantidad de tramas cursadas por los puntos de acceso en la Red Laptops durante una semana de lunes a domingo.

En esta red (Fig 45), obviamente ocurre lo mismo que con la red Internet. Pero en este caso, se aprecia qué la mayoría del tráfico es cursado por en punto de acceso con dirección física BSSID-6, ya que es el más próximo a la Raspberry.

3.2. Escenario 2

En este escenario se ha incluido la funcionalidad de poder detectar si un usuario se ha estado moviendo, para poder realizar un estudio más completo.

Las principales características de este escenario son las siguientes:

Periodo	26 Julio – 20 Agosto
Ventana temporal	1h
Número de dispositivos totales	331
Número de puntos de acceso totales	9
Número de redes	3

Tabla 10: Características escenario 2.

Se monitorizan 3 redes simultáneamente:

- Red 1: Red Laptops, 121 usuarios detectados.
- Red 2: Red Internet, 210 usuarios detectados.
- Red 3: Red Guests.

El análisis se centrará en las redes laptops e internet, debido a que los datos obtenidos en la red guests no son suficientes para sacar ningún tipo de conclusión.

3.2.1. Análisis de comportamiento general en el escenario 2

Los puntos de acceso detectados en las 3 redes se muestran en la siguiente tabla.

STA_Status	DIA_I	HORA_I	SSID	BSSID	Fabricante	Channel_AP	SSI_signal
Access Point	26/07/17	09:52:34	GUEST	BSSID-1	Hewlett Packard	1	-61
Access Point	26/07/17	09:52:34	Laptop_Corp	BSSID-2	Hewlett Packard	1	-60
Access Point	26/07/17	09:52:34	INTERNET	BSSID-3	Hewlett Packard	1	-62
Access Point	26/07/17	09:53:29	INTERNET	BSSID-4	Hewlett Packard	6	-62
Access Point	26/07/17	09:53:29	GUEST	BSSID-5	Hewlett Packard	6	-62
Access Point	26/07/17	09:53:29	Laptop_Corp	BSSID-6	Hewlett Packard	6	-61
Access Point	26/07/17	09:53:29	INTERNET	BSSID-7	Hewlett Packard	11	-62
Access Point	26/07/17	09:53:29	GUEST	BSSID-8	Hewlett Packard	11	-62
Access Point	26/07/17	09:53:29	Laptop_Corp	BSSID-9	Hewlett Packard	11	-61
Access Point	08/08/17	08:46:29	INTERNET	BSSID-10	Hewlett Packard	1	-66
Access Point	10/08/17	15:55:32	INTERNET	BSSID-11	Hewlett Packard	1	-69
Access Point	17/08/17	09:04:43	GUEST	BSSID-12	Hewlett Packard	1	-66

Figura 46: puntos de acceso detectados.

En esta tabla se pueden observar los diferentes campos de la tabla donde están almacenados los puntos de acceso, la hora a la que fueron detectados, el día, a que red pertenecen, su dirección MAC, fabricante, canal por el que están transmitiendo y señal con la cual es recibida la trama. Los 9 primeros puntos de acceso, detectados el día 26/07/17, y aproximadamente a la misma hora son los que están ubicados en la planta de oficinas monitorizada. Los tres últimos son puntos de acceso de otras plantas, detectados por la Raspberry debido a que alguna trama generada por dichos puntos de

acceso llegó a ella de forma casual como podemos deducir por los diferentes días y horas a las que se detectaron.

Fabricante	Usuarios
Apple Inc.	48
ASUSTek COMPUTER INC.	19
BQ	32
China Palms Telecom.Ltd	1
HUAWEI TECHNOLOGIES CO.LTD	6
Intel Corporate	2
LG Electronics Mobile Communications	2
LONGCHEER TELECOMMUNICATION LIMITED	1
Murata Manufacturing Co. Ltd.	1
OnePlus Tech Shenzhen Ltd	3
OnePlus Technology Shenzhen Co. Ltd	1
SAMSUNG ELECTRO-MECHANICSTHAILAND	19
Samsung Electronics Co.Ltd	49
Shenzhen TINNO Mobile Technology Corp.	4
Sony Mobile Communications AB	16
WISOL	2
Xiaomi Communications Co Ltd	3
zte corporation	1
Total general	**210**

Tabla 11: donde se observa el número y fabricante de los dispositivos utilizados por los usuarios en la Red Internet.

En la red Internet se detectaron un total de 210 dispositivos que en algún momento estuvieron cursando tráfico en la red. Al igual que en el escenario 1, se puede deducir por la marca de los dispositivos que a esta red se conectan smartphones, tablets, impresoras, etc.

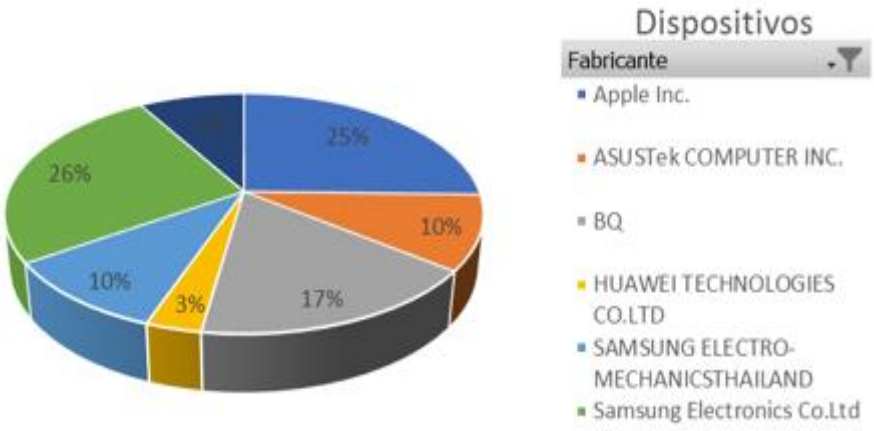


Figura 47: Gráfico con porcentaje de dispositivos detectados en la red Internet según su marca.

Apple Inc.	2
ASUSTek COMPUTER INC.	2
BQ	3
HTC Corporation	1
Intel Corporate	112
Samsung Electronics Co.Ltd	1
Grand Total	121

Tabla 12: Número y fabricante de los dispositivos utilizados por los usuarios en la Red Laptops.

En la red Laptops hay un total de 121 dispositivos cursando tráfico en esta red, de los cuales su gran mayoría son laptops corporativos.

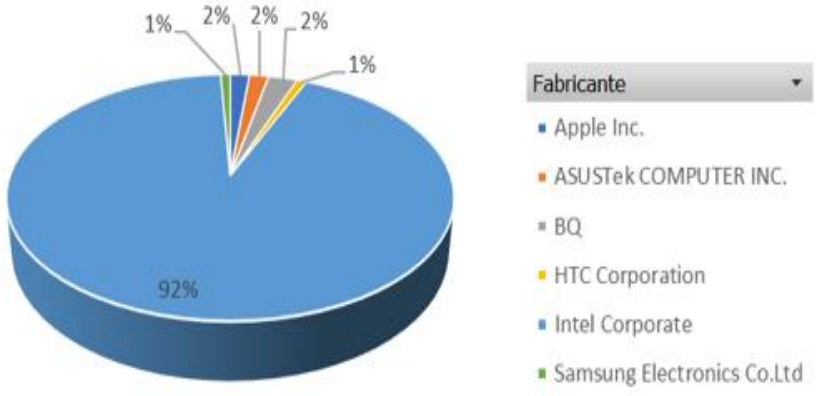


Figura 48: Gráfico con porcentaje de dispositivos detectados en la red Laptops según su marca.

3.2.2. Análisis de comportamiento según la presencia de los dispositivos

Para poder determinar la presencia de los usuarios en la oficina se realizarán mediante consultas a la base de datos, un análisis por día de la presencia de los usuarios que estuvieron en algún momento conectados a las redes monitorizadas.

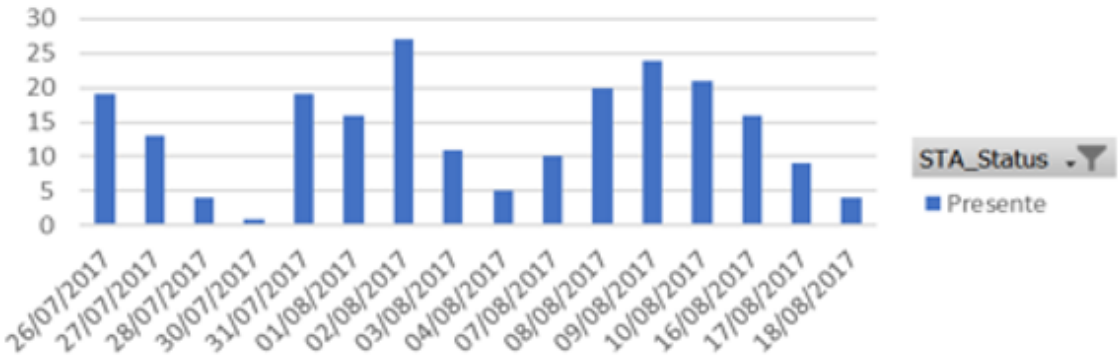


Figura 49: Gráfica que muestra la presencia de los usuarios por días en la red Laptops.

En la figura 49 se considera presente aquellos dispositivos que han recibido o transmitido tramas de datos durante ese día. Se observa que los fines de semana no hay dispositivos presentes, dichos días ni siquiera aparecen en la gráfica. Además, los viernes el número se ve reducido considerablemente comparado con el resto de días laborables de la semana, esto se debe a que muchos usuarios teletrabajan el viernes.

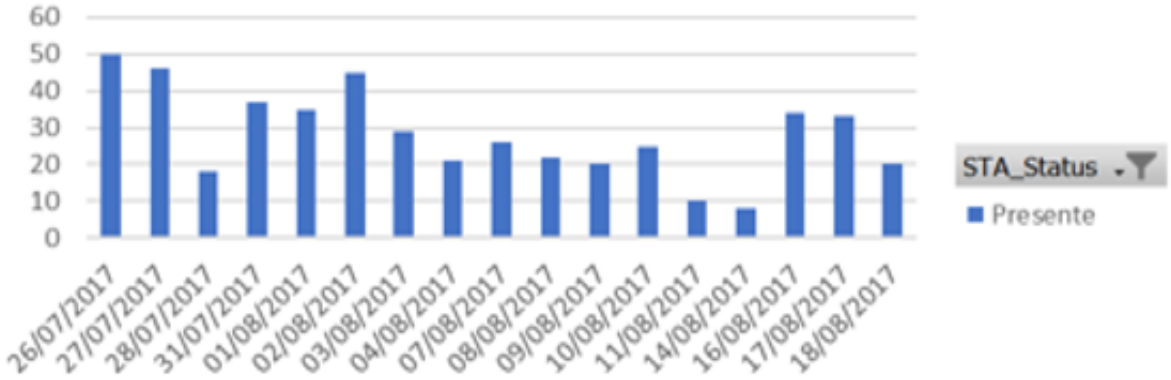


Figura 50: Gráfica que muestra la presencia de los usuarios por días en la red Internet.

En la figura 50 se puede comprobar que el número de dispositivos detectados en la red Internet es mayor que número de dispositivos detectados en la red Laptops. Se puede deducir que esto es debido a que las personas se mueven por las diferentes plantas del edificio, al moverse suelen llevar consigo sus teléfonos móviles mientras que su laptop corporativo lo dejan en su puesto de trabajo. Entonces al moverse a una planta que no es donde se encuentra su puesto de trabajo con el teléfono móvil, este se conecta a la red de dicha planta y la Raspberry lo detecta como un nuevo usuario.

3.2.3. Análisis de la presencia según patrones de presencia

Para poder sacar conclusiones más relevantes en cuanto a la presencia de los dispositivos, se va a estudiar la presencia de los mismos mediante patrones de presencia, es decir, se busca que dispositivos estuvieron presentes en la oficina los mismos días durante el periodo de monitorización. De esta manera, se sacarán conclusiones como que usuarios pueden pertenecer a un mismo equipo de trabajo. Estos patrones se consiguen mediante un script de Python, con el que se hacen consultas a la base de datos.

En este análisis se ha considerado como patrón de presencia los días que al menos dos dispositivos han coincidido en la oficina. Por ejemplo, el patrón 17:

Patron17	
SSID-1	2
SSID-2	1

Figura 51: Patrón de presencia 17.

Se tiene que hubo 2 dispositivos que estuvieron presentes los mismos días en la oficina en la red SSID-1 y otro dispositivo que también estuvo presente esos mismos días pero en la SSID-2.

En concreto, los días que estuvieron presentes esos 3 dispositivos en la oficina fueron:

DIA_U	STA_Status	Movil AP	STA_mov
02/08/17	Presente	Fijo	Fijo
03/08/17	No presente	Fijo	Fijo
04/08/17	Presente	Fijo	Fijo
05/08/17	No presente	Fijo	Fijo
06/08/17	No presente	Fijo	Fijo
07/08/17	Presente	Fijo	Fijo
08/08/17	Presente	Fijo	Fijo
09/08/17	No presente	Fijo	Fijo
10/08/17	Presente	Fijo	Fijo
11/08/17	No presente	Fijo	Fijo
12/08/17	No presente	Fijo	Fijo
13/08/17	No presente	Fijo	Fijo
14/08/17	No presente	Fijo	Fijo
15/08/17	No presente	Fijo	Fijo
16/08/17	Presente	Fijo	Fijo
17/08/17	Presente	Fijo	Fijo
18/08/17	No presente	Fijo	Fijo
19/08/17	No presente	Fijo	Fijo
20/08/17	No presente	Fijo	Fijo
21/08/17	No presente	Fijo	Fijo

Tabla 13: Patrón de presencia 17 desglosado en días.

Se ha realizado este estudio con todos los dispositivos detectados y durante todos los días de la monitorización, el resultado ha sido el siguiente:

Patron de Presencia	Nº Dispositivos	Patron de Presencia	Nº Dispositivos	Patron de Presencia	Nº Dispositivos
Patron0		Patron18		Patron29	
SSID-1	8	SSID-1	4	SSID-1	2
SSID-2	15	Patron19		Patron3	
Patron1		SSID-1	2	SSID-2	2
SSID-1	2	SSID-2	5	Patron30	
SSID-2	9	Patron2		SSID-1	2
Patron10		SSID-1	1	SSID-2	4
SSID-2	5	SSID-2	4	Patron31	
Patron11		Patron20		SSID-1	2
SSID-2	2	SSID-1	1	Patron32	
Patron12		SSID-2	3	SSID-1	2
SSID-1	3	Patron21		SSID-2	1
SSID-2	1	SSID-1	1	Patron33	
Patron13		SSID-2	3	SSID-1	2
SSID-1	2	Patron22		SSID-2	7
SSID-2	5	SSID-1	2	Patron34	
Patron14		Patron23		SSID-2	2
SSID-1	1	SSID-2	2	Patron4	
SSID-2	4	Patron24		SSID-2	2
Patron15		SSID-2	2	Patron5	
SSID-1	5	Patron25		SSID-1	4
SSID-2	4	SSID-2	4	SSID-2	7
Patron16		Patron26		Patron6	
SSID-1	7	SSID-2	3	SSID-1	5
SSID-2	9	Patron27		SSID-2	15
Patron17		SSID-1	2	Patron7	
SSID-1	2	Patron28		SSID-2	2
SSID-2	1	SSID-1	2	Patron8	
		SSID-2	3	SSID-2	2
				Patron9	

Tabla 14: Patrón de presencia total.

3.2.4. Análisis de comportamiento según el movimiento de los dispositivos

Se va realizar un análisis para comprobar si los dispositivos se están moviendo o permanecen fijos durante los intervalos de monitorización, para ello se van a tener en cuenta dos premisas:

- Si el dispositivo ha cambiado de punto de acceso al cual estaba conectado a través del cual cursaba tráfico en la red en algún momento durante el intervalo. Por tanto, si se detecta que el punto de acceso es diferente se considerará que se ha movido, debido a que al haberse conectado a otro punto de acceso el usuario se ha tenido que mover en algún momento alrededor de la oficina.
- Si la Raspberry recibe tramas cursadas por un dispositivo en concreto con una diferencia de señal de al menos 30 dbm, se considerará que el usuario se ha estado moviendo y por esa razón se reciben las tramas con una señal mayor o menor.

Para el análisis se han tenido las siguientes consideraciones a la hora de mostrar los resultados gráficamente, se han utilizado 3 estados (1º estado -2º Estado – 3º Estado):

- 1º Estado: En este estado se medirá si el dispositivo ha cambiado de punto de acceso al cual estar vinculado durante el día. Los posibles valores de este estado son:
    a. Moving: El dispositivo ha cambiado de punto de acceso al cual estar conectado durante el día.
    b. Static: El dispositivo no ha cambiado de punto de acceso al cual estar vinculado durante el día.
- 2º Estado: En este estado se medirá si ha habido variaciones de potencia de la señal con la cual se han recibido las tramas:
    a. Moving: Detectado variaciones de potencia de las tramas recibidas durante el periodo de intervalo de comportamiento (1 hora) **mayor** a 30dbm.
    b. Static: Las variaciones de potencia con las que se detectan las tramas recibidas durante el intervalo de comportamiento es **menor** a 30dbm.
- 3º Estado: Simplemente es para asegurarse que el dispositivo analizado ha transmitido tramas de datos durante el intervalo de comportamiento, es decir, se mira si el dispositivo ha estado presente en alguno de los 24 intervalos que tiene el día.

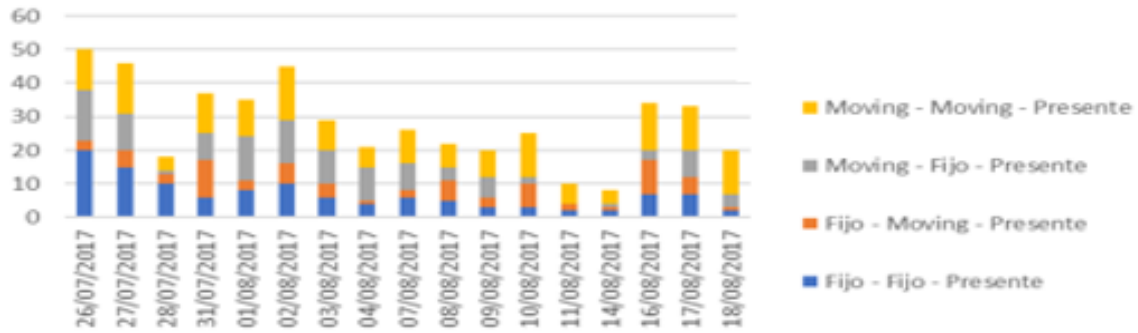


Figura 52: Comportamiento de los dispositivos según el movimiento en la red Internet.

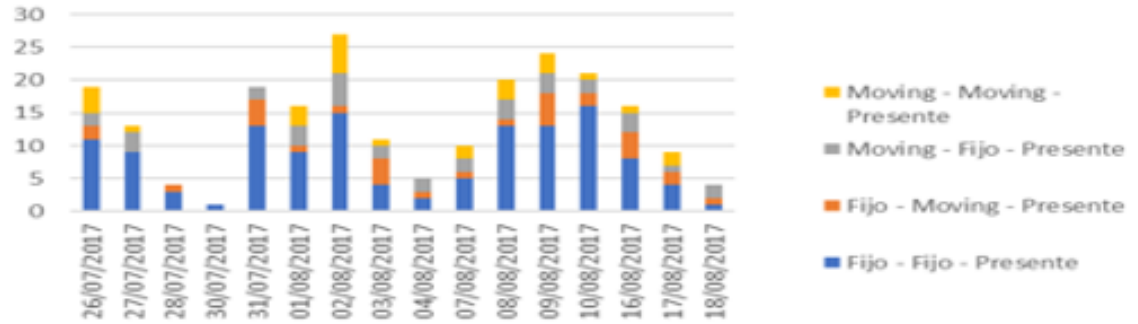


Figura 53: Comportamiento de los dispositivos según el movimiento en la red Laptop.

Observando las figuras 52 y 53, se ve claramente que en la red Internet (fig 52) el número de dispositivos móviles que se están moviendo durante el día es bastante más numeroso, que en la red de la laptop (fig 53), en la cual la mayor parte del tiempo están estáticos. Si esta funcionalidad se hubiese probado en áreas públicas o recintos comerciales, con varios equipos monitorizando tendríamos por día y hora las áreas del recinto donde hay más movimientos de usuarios y si usuario en concreto se ha movido o ha salido del recinto.

3.2.5. Análisis de tráfico cursado por las redes

Se va a analizar la cantidad de tráfico cursado por las redes monitorizadas. Para poder sacar conclusiones del tipo de tráfico cursado por las redes se van a tener en cuenta los campos de longitud de las tramas:

- Tramas de longitud LONG4: Son las tramas de tamaño de 100 a 300 bytes.
- Tramas de longitud LONG3: Son las tramas de tamaño de 300 a 500 bytes.
- Tramas de longitud LONG2: Son las tramas de tamaño de 500 a 1000 bytes.
- Tramas de longitud LONG1: Son las tramas de tamaño de más de 1000 bytes.

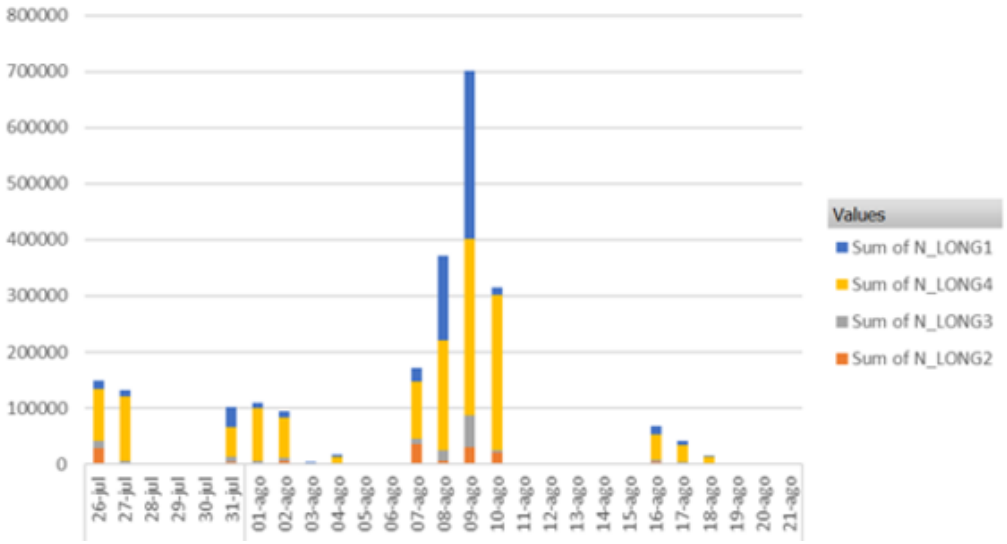


Figura 54: Gráfica con la cantidad y tipo de tráfico cursado en la red Laptop.

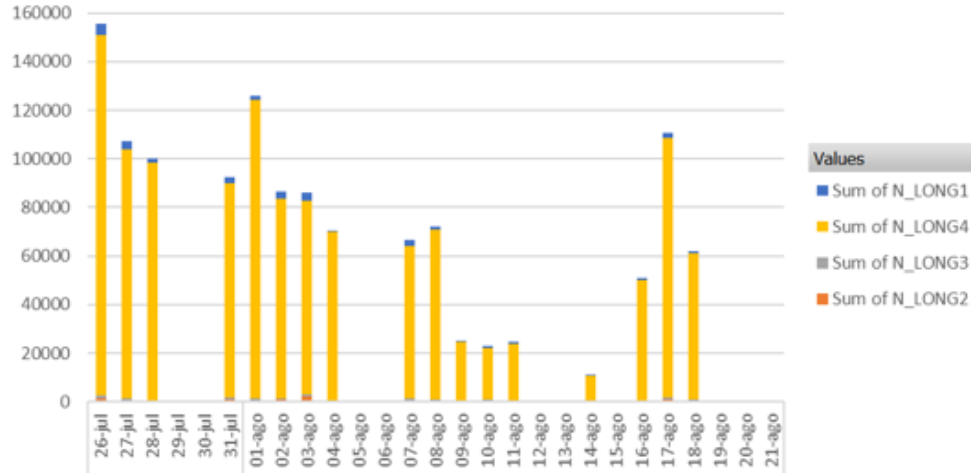


Figura 55: Gráfica con la cantidad y tipo de tráfico cursado en la red Internet.

Se vuelve a observar el mismo comportamiento que en escenario 1, es decir, los dispositivos en la red Internet cursan un tipo de tráfico donde la mayoría de tramas son de tamaño menor a 300 bytes. Mientras que en la red laptops tenemos mayor variación en el tamaño de tramas, algunos días se ve un tráfico de tamaño de tramas por encima de 1000 bytes bastante significativo.

CAPÍTULO IV

4.CONCLUSIONES Y FUTURAS LÍNEAS DE TRABAJO

4.1. Conclusiones

El objetivo inicial de este trabajo era desarrollar un sistema de escanear redes inalámbricas tomando como referencia herramientas comerciales como Fing. Con dicho escaneo se debería poder analizar el comportamiento de los usuarios de la red monitorizada, cómo por ejemplo, encontrar patrones de comportamiento comunes entre los diferentes usuarios.

En la primera fase de investigación de las herramientas que escaneaban redes inalámbricas, el estudio se enfocó en la aplicación Fing, se estudió su manejo y las posibilidades que daba para el análisis posterior. Se procedió a desarrollar un programa en Python muy básico que generara ARP spoofing y detectara que dispositivos estaban conectado a la red monitorizada.

Se exploraron otras aplicaciones como Airodump-ng, TCPdump para ver el potenciar que tenían para el objetivo inicial, y aunque hay una gran variedad de dichas aplicaciones, se decidió desarrollar un sniffer propio en el lenguaje Python con el objetivo de monitorización de tráfico y almacenar solamente aquella información necesaria para nuestro análisis.

El objetivo del análisis era tener la información de estado de cada dispositivo en tiempo real del comportamiento con respecto al tráfico de datos. El desafío más importante que se encontró fue optimizar la programación y el intervalo de tiempo para hacer el análisis y que no afectara a la latencia del sniffer. La elección del intervalo dependerá del tamaño de la/s red/s a monitorizar en cuanto a usuarios ya que obviamente el tiempo proceso pare el análisis está directamente afectado por este número.

En principio, se pensó en hacer la monitorización con un laptop y posteriormente se pensó que el hacer la monitorización con una Raspberry PI3 abría la posibilidad de extender el proyecto hacía la monitorización de áreas mayores ya que se podría desplegar varias unidades cubriendo los puntos de acceso de la red WIFI.

Una vez depurado el programa y tras varias pruebas, se dejó monitorizando en una planta de oficinas con capacidad de 90 puestos de trabajos, donde la mayoría de ellos no

están reservados, ya que los empleados pueden hacer uso del teletrabajo varios días por semana. Esta monitorización fue de dos meses en tandas de un mes. Este ejercicio se vió muy interesante ya que en el análisis se podía observar los días y horas de más afluencias de empleados en la oficina y que días se hacía más teletrabajo, asi como la distribución del tráfico en las dos redes monitorizadas.

El trabajo debería haberse completado con varias Raspberries monitorizando la planta de ofician y de ese modo el análisis de movilidad de los empleados por la planta habría sido completo.

4.2. Futuras líneas de trabajo

En este apartado se van a enumerar propuestas para posibles mejoras que puedan llevarse a cabo partiendo de este sistema.

- Incluir **monitorización activa** junto con la pasiva en aquellas redes donde tengamos acceso, para poder hacer una comparación en la fase de análisis de ambos resultados.

- Monitorización con **varias Raspberry Pi**, teniendo una cobertura total de las áreas. **Incluir en el sistema un servidor** el cual se pudiese comunicar con todas las Raspberries de forma que todos los datos capturados por las raspberries quedasen almacenados en dicho servidor.

- Implementación web donde se pueda visualizar gráficas en tiempo real de los dispositivos conectados, y de la cantidad de tramas de datos por intervalo y por red monitorizada.

- Implementar un **sistema almacenamiento** y gestión de los datos de las diferentes Raspberry Pi. El tráfico debería ser capturado y almacenado en tiempo real, se tendría que usar un protocolo para capturar rápidamente y con baja latencia.

La idea final sería ampliar el alcance del proyecto y poder abarcar una monitorización de redes WIFI grandes, para crear una “Dashboard” que muestre los dispositivos móviles identificados alrededor de la Raspberry, de este modo se podría analizar el tráfico para ver la actividad de los usuarios (áreas de compras, en zonas urbanas, etc,) en el área de cobertura, para ello sería necesario incluir las ideas anteriores. [21]

A. ANEXOS

A.1. PRESUPUESTOS

• **Autor:** Vicente Gaitán Garrido

• **Departamento de Ingeniería Telemática**

• **Descripción del Proyecto**

- **Título:** Monitorización y análisis de redes inalámbricas 802.11
- **Duración:** 6 meses

• **Presupuesto total del Proyecto:** ver tablas

• **Subcontratación de tareas:** No se especifica

• **Otros costes indirectos:** No se especifica

En las siguientes tablas se puede observar la planificación del presupuesto destinado y gastado en la plantilla y los materiales utilizados para su consecución, así como gráficas que ilustran los resultados.

ESTADO	MATERIALES	PRESUPUESTO	REAL	DIFERENCIA (EUR)	DIFERENCIA (%)
▲	Ordenador portatil	780,00 €	565,00 €	215,00 €	28%
▲	Monitor 17"	125,00 €	50,00 €	75,00 €	60%
▬	Teclado Externo	10,00 €	10,00 €	0,00 €	0%
▲	Raspberry PI 3	120,00 €	40,00 €	80,00 €	67%
▲	Antena externa TL-WN722N (1	30,00 €	10,00 €	20,00 €	67%
▬	Conexión Internet	180,00 €	180,00 €	0,00 €	0%
▲	Gastos totales	1.245,00 €	855,00 €	390,00 €	31%

Tabla 15: Presupuestos de los materiales.

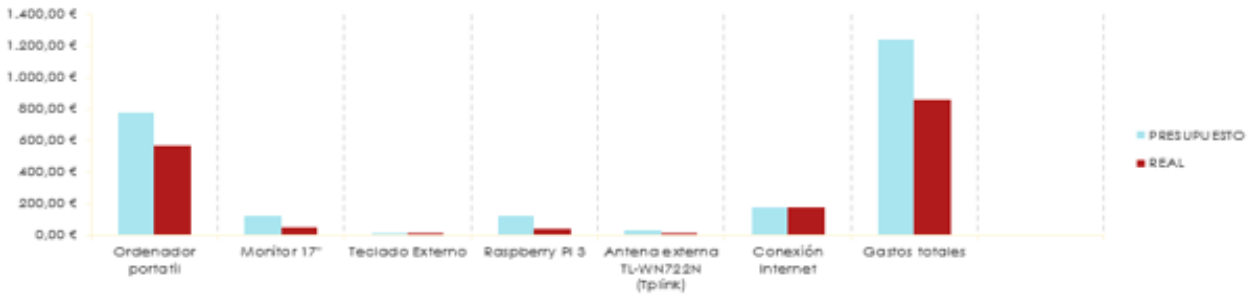


Figura 56: Gráfica que ilustra los presupuestos de los materiales.

ESTADO	OPERACIÓN	PRESUPUESTO	REAL	DIFERENCIA (EUR)	DIFERENCIA (%)
	Ingeniero Graduado (6 meses)	7.200,00 €	7.200,00 €	0,00 €	0%
	x2Ingeniero Senior (2 meses)	7.600,00 €	5.600,00 €	2.000,00 €	26%
	Otros			0,00 €	
	Gastos totales	**14.800,00 €**	**12.800,00 €**	**2.000,00 €**	**14%**

Tabla 16: Presupuestos de la plantilla.

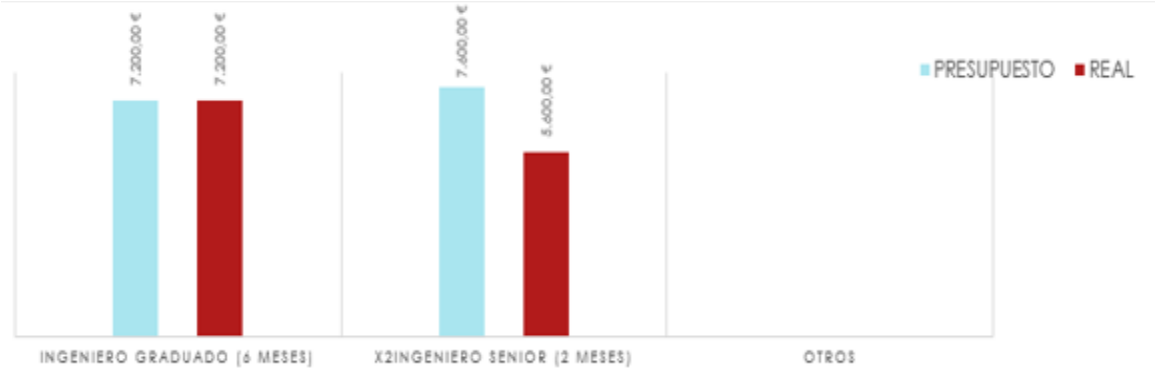


Figura 57: Gráfica que ilustra los presupuestos de la plantilla.

En conclusión, el total del presupuesto destinado a este proyecto ha sido:

	PRESUPUESTO	REAL	DIFERENCIA(EUR)	DIFERENCIA(%)
TOTALES	16.045,00 €	13.655,00 €	2.390,00 €	14%

Figura 58: Presupuesto total

A.2. PLANIFICACIÓN TEMPORAL

Para mostrar la planificación seguida de las tareas más importantes con una estimación del tiempo que se ha empleado para la consecución del proyecto se ha realizado la siguiente tabla.

Nombre Tarea	Fecha de Inicio	Fecha Final	Duración	Horas
Inicio	15-feb	26-feb	11 días	22 horas
Inmersión	02-mar	20-mar	18 días	36 horas
Elaboración	04-abr	20-may	46 días	138 horas
Monitorización I	28-may	01-jul	33 días	
Análisis I	04-jul	15-jul	11 días	44 horas
Monitorización II	26-jul	20-ago	25 días	
Análisis II	24-ago	03-sep	10 días	40 horas
Documentación	04-sep	24-sep	20 días	100 horas

Tabla 17: Planificación temporal.

Con estos datos se ha realizado un diagrama más detallado del tiempo empleado.

Figura 59: Diagrama planificación temporal.

A.3. IMPACTO SOCIAL Y APLICACIONES

La función principal de este proyecto es la monitorización y análisis de redes inalámbricas, por tanto, se maneja gran cantidad de datos.

Estos datos pueden utilizarse de diferentes maneras, como un modo de lograr una ventaja competitiva en el mundo empresarial, para generar un conocimiento diferencial a la hora de tomar determinadas decisiones. En una compañía, por ejemplo, se puede utilizar para saber en que zonas hay más afluencia de usuarios y de esta manera mejorar la infraestructura de la misma para conseguir un mejor servicio, si el horario laboral es flexible, este proyecto podría servir para estimar las horas a las que mayoritariamente los empleados acuden a la oficina, etc. Estos mismos datos extraídos a partir del comportamiento de los empleados de una empresa pueden ser usados por los comercios o restaurantes para de esta manera saber en que franja horaria pueden necesitar más personal debido a que mayoritariamente las personas salen de sus trabajos y tienen más disponibilidad de dedicar tiempo a ocio o compras. De igual manera, si se hiciese el estudio en un centro comercial se podría saber a en que franja horaria hay más afluencia de personas e incluso en que zona del centro comercial se localizan para con esta información tomar estrategias corporativas.

Por otro lado, éticamente supone un gran problema de privacidad ya que con este tipo de herramientas se puede tener información sobre el comportamiento de las personas, incluso si se tiene acceso a la dirección MAC de los dispositivos se podría seguir indagando y sacar mucha información como el nombre del dueño un dispositivo, domicilio, etc.

Debido a todo esto, se puede incluir las características de este proyecto dentro de ‘’Big Data’’, con todos los pros y los contras que conlleva. Con esta tecnología se pueden identificar y mejorar aspectos de la sociedad vulnerables, o por otro lado, se pueden identificar estos mismos aspectos y explotar malintencionadamente estas vulnerabilidades. La tecnología Big Data no es positiva ni negativa por si misma, depende de cómo sea usada, por ello es muy importante que se proteja la privacidad de la información y se asegure el cumplimiento de la legislación vigente. [23]

BIBLIOGRAFÍA

[1] J. F. Kurose, K.W Ross, “Redes de Computadores. Un Enfoque Descendente Basado en Internet”, Pearson S.A, 2003.

[2] Techtarget. Search data center en español

http://searchdatacenter.techtarget.com/es/consejo/LAN-inalambrica-o-Ethernet-Una-comparacion-de-costos-de-manzanas-con-manzanas

[3] ABI Research

https://www.abiresearch.com/

[4] Cisco

http://globalnewsroom.cisco.com/es/es/release/El-tr%C3%A1fico-global-de-datos-m%C3%B3viles-se-multiplicar%C3%A1-por-siete-entre-2016-y-2021-2475531

[5] Cisco II

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html?CAMPAIGN=Mobile+VNI+2017&COUNTRY_SITE=us&POSITION=Press+Release&REFERRING_SITE=PR&CREATIVE=PR+to+MVNI+white+paper#AnalyzingtheExpandingRole

[6] Wifi Alliance

https://www.wi-fi.org/

[7] Organizaciones certificadoras y reguladoras inalámbricas

https://es.wikipedia.org/wiki/Organizaciones_Certificadoras_y_Reguladoras_Inal%C3%A1mbricas

[8] Estándares inalámbricos

http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf

[9] Aspectos legislativos y despliegue de redes Wi-Fi.

http://bibing.us.es/proyectos/abreproy/11761/fichero/Volumen1%252F8-Cap%C3%ADtulo4+-+Aspectos+legislativos+y+despliegue+de+redes+WIFI.pdf+

[10] LOPD

http://www.mundolopd.com/lopd/

[11] Monitoreo de redes

https://blog.pandorafms.org/es/herramientas-de-monitoreo-de-redes/

[12] Python

https://www.python.org/

https://courses.edx.org/courses/course-v1:UTAx+CSE1309x+2016T1/course/

https://pybonacci.wordpress.com/tag/tutorial-matplotlib-pyplot/

[13] 802.11® Wireless Networks: The Definitive GuideBy Matthew Gast

[14] Ubuntu

https://help.ubuntu.com/

[15] Aircrack-ng

https://www.aircrack-ng.org/

[16] Wireshark

http://www.wireshark.org

[17] Ubuntu-MATE

https://ubuntu-mate.org/raspberry-pi/

[18] SQLite3

https://docs.python.org/2/library/sqlite3.html

http://python-para-impacientes.blogspot.com.es/2014/02/bases-de-datos-sqlite3.html

[19] ARP Protocol Cisco

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/15-mt/arp-15-mt-book/arp-config-arp.html

[20] Reinicio automático

https://nideaderedes.urlansoft.com/2013/12/20/como-ejecutar-un-programa-automaticamente-al-arrancar-la-raspberry-pi/

[21] Mejoras

https://holisticsecurity.io/2016/02/02/everything-generates-data-capturing-wifi-anonymous-traffic-raspberrypi-wso2-part-i/

[22] AP: Punto de Acceso.

[23]Big Data

https://www.oracle.com/big-data/index.html